

SÉRIE PENSAMENTO MATEMÁTICO @ CIÊNCIA DA COMPUTAÇÃO

**Volume III: Computação Quântica: Aspectos Físicos e Matemáticos - Uma Abordagem Algébrica**

*Planck*

*Schrödinger*

*Einstein*

*Neils Bohr*

*Von Neumann*

*Heisenberg*

*Deutsch*

*Feynman*

*Dirac*

*Pauli*

*Benioff*

*Shor*

João Bosco M. Sobral

EDIÇÃO DO AUTOR

João Bosco M. Sobral  
Renato Bobsin Machado



*Computação Quântica:  
Aspectos Físicos e Matemáticos - Uma  
Abordagem Algébrica*

Série Pensamento Matemático @ Ciência da Computação

Laboratório e Grupo de Pesquisa  
UFSC-CNPq



Universidade Federal de Santa Catarina  
Centro Tecnológico  
Departamento de Informática e Estatística  
Laboratório DMC & NS  
Projeto de Pesquisa Sispex-UFSC 2016.11146  
- Universidade do Oeste do Estado do Paraná - UNIOESTE -



João Bosco M. Sobral  
Renato Bobsin Machado

*Computação Quântica:  
Aspectos Físicos e Matemáticos - Uma  
Abordagem Algébrica*

Série Pensamento Matemático @ Ciência da Computação

**1ª Edição**  
Florianópolis  
João Bosco Mangueira Sobral  
2019

© 2019 João Bosco M. Sobral  
Renato Bobsin Machado  
**Universidade Federal de Santa Catarina**  
**Centro Tecnológico**  
**Departamento de Informática e Estatística**  
**Laboratório DMC & NS**  
**Projeto de Pesquisa Sigpex-UFSC 2016.11146**  
**- Universidade do Oeste do Estado do Paraná - UNIOESTE -**

Qualquer parte desta publicação pode ser reproduzida, desde que citada a fonte, e as fontes originais referenciadas neste livro.

Além da bibliografia citada, o autor fez uso extensivo de diversos e excelentes sites da Internet, e imagens dos personagens e fatos marcantes na história da Matemática, da Lógica e da Ciência da Computação, aos quais, não sendo de sua propriedade, estão devidamente referenciados. Conforme declarado à Agência Brasileira do ISBN, este livro não é para ser comercializado.

**Nota** - Muito trabalho foi empregado nesta edição. No entanto, podem ocorrer erros de digitação, impressão ou dúvida sobre os conceitos. Em qualquer das hipóteses, o autor e editor, solicita a comunicação nos emails *bosco.sobral@ufsc.br* ou *jbmsobral@gmail.com*, para que o mesmo possa corrigir o ponto mencionado.

**Catálogo na fonte pela Biblioteca Universitária da  
Universidade Federal de Santa Catarina**

S677c

Sobral, João Bosco Mangueira  
Computação quântica [recurso eletrônico] : aspectos físicos e matemáticos : uma abordagem algébrica / João Bosco Mangueira Sobral, Renato Bobsin Machado. – Dados eletrônicos. – Florianópolis : ine/CTC/UFSC, 2019.

320 p. : ils., tabs. - (Série Pensamento Matemático @ Ciência da Computação)

Inclui bibliografia.

E-book (PDF)

ISBN 978-85-902995-4-7

1. Computação - Matemática. 2. Computação quântica. I. Machado, Renato Bobsin. II. Série.

CDU: 519.6

Elaborado por Jonathas Troglio – CRB-14/1093

# Agradecimentos

- Ao Prof. **João Cândido Dovicchi**, que originou o tema no INE e sempre cultivando a computação quântica, se prontificou a colaborar no prefácio deste livro.
- Ao Prof. **Roberto Willrich** (INE-UFSC), pela compreensão nos momentos que precisei renovar o prazo de término deste trabalho no Sigpex-UFSC.
- Às Profas. **Silvia Modesto Nassar** e **Clara Amélia de Oliveira**, que em fevereiro/1978, acreditaram e confiaram na minha jornada na UFSC.

## In memoriam

No término de minha carreira no INE-CTC-UFSC, aos saudosos colegas professores:

- **Alceu Ribeiro Alves** (INE-UFSC),
- **Bernardo Gonçalves Riso** (INE-UFSC),
- **Jorge Muniz Barreto** (INE-UFSC),
- **Raul Guenther** (Laboratório de Robótica, EMC-UFSC),
- **Sérgio Villas-Boas** (Escola Politécnica-UFRJ),

que certamente, se estivessem conosco, gostariam de conhecer e melhorar este livro.



# Lista de ilustrações

Figura 1 – Galileu Galilei - por Justus Sustermans 1636. . . . .	2
Figura 2 – Christiaan Huygens - Em 1690, desenvolveu uma ampla teoria das ondas da luz. . . . .	3
Figura 3 – Newton - Retrato por Godfrey Kneller, 1689, com 46 anos de idade. . . . .	4
Figura 4 – Issac Newton - Sua obra, <i>Princípios Matemáticos da Filosofia Natural</i> é considerada uma das mais influentes na história da ciência. . . . .	4
Figura 5 – Ampère - Fez importantes contribuições para o estudo do eletromagnetismo. . . . .	5
Figura 6 – Thomas Young - Juntamente com Fresnel demonstrou várias deficiências da teoria corpuscular da luz. . . . .	5
Figura 7 – Augustin Fresnel - Trabalhando com Young, demonstrou várias deficiências da teoria corpuscular da luz, que podem ser resolvidas assumindo ondas de luz, transversal, em um meio universal chamado Ether. . . . .	6
Figura 8 – Charles - A um volume constante, a pressão de uma determinada massa de gás é diretamente proporcional à sua temperatura absoluta. . . . .	7
Figura 9 – Orsted - A ligação entre eletricidade e magnetismo. . . . .	7
Figura 10 – Carnot e Primeira Lei da Termodinâmica - Nos processos físicos a energia não se perde, ela se converte em um outro tipo de energia. . . . .	8
Figura 11 – Faraday - Um pioneiro no estudo da eletricidade e magnetismo e descobridor da indução eletromagnética. . . . .	9
Figura 12 – Johann Balmer - O primeiro indício da "revolução quântica" surgiu em 1885 com Balmer. . . . .	10
Figura 13 – James Joule - A equivalência entre trabalho e calor. . . . .	11
Figura 14 – Rudolf Clausius - Introduziu o conceito de entropia, a medida da quantidade de energia térmica que não pode ser revertida em energia mecânica. . . . .	11
Figura 15 – Lord Kelvin - Complementou as pesquisas de Carnot sobre a irreversibilidade dos processos termodinâmicos, dando origem às bases da Segunda Lei da Termodinâmica. . . . .	12
Figura 16 – Kirchhoff - O pioneiro no estudo da emissão de radiação de um corpo negro. . . . .	13
Figura 17 – Maxwell - É mais conhecido por ter dado forma final à teoria moderna do eletromagnetismo, que une a eletricidade, o magnetismo e a óptica. . . . .	15
Figura 18 – John Strutt - as evidências de inconsistências entre trabalhos experimentais e o modelos matemáticos clássicos utilizados. . . . .	16
Figura 19 – Jozef Stefan - Em 1879 estabeleceu que a radiação total de um corpo negro é proporcional à quarta potência de sua temperatura. . . . .	16



Figura 20 – Lei de Stefan-Boltzmann - A <i>potência</i> total da radiação emitida (a área sob a curva) aumenta com a temperatura. . . . .	17
Figura 21 – Ludwig Boltzmann aos 24 anos em 1869 - Leis da radiação de um corpo negro, juntamente com Jozef Stefan. . . . .	18
Figura 22 – Rydberg - A previsão dos comprimentos de onda da radiação de fótons. . . . .	18
Figura 23 – Fórmula de Rydberg - Um pedaço do documento original que detalha a fórmula de Rydberg. . . . .	19
Figura 24 – Rydberg - O trabalho sobre espectros de emissão de metais alcalinos.	19
Figura 25 – Wilhelm Wien - A intensidade máxima da radiação de um corpo negro desloca-se para comprimentos de onda menores e frequências maiores. . . . .	20
Figura 26 – J. J. Thomson - O descobridor do elétron em 1897. . . . .	20
Figura 27 – Lummer em 1902 - Primeiras medidas de energia emitida por um corpo negro. . . . .	21
Figura 28 – Pringshein - Juntamente com Lummer, as primeiras medidas de energia emitida por um corpo negro. . . . .	22
Figura 29 – Fórmula de Rayleigh-Jeans para mostrar a distribuição espectral de um corpo negro. . . . .	24
Figura 30 – John William Strutt - Prêmio Nobel de Física em 1904. . . . .	24
Figura 31 – James Jeans - Ajudou a descobrir a lei de Rayleigh-Jeans. . . . .	25
Figura 32 – Fórmula de Rayleigh-Jeans mostrando a catástrofe ultravioleta quanto a distribuição espectral de um corpo negro. . . . .	25
Figura 33 – Mark Planck - Explicou a emissão de radiação do corpo negro. . . . .	30
Figura 34 – Marx Planck - introduziu o conceito de energia quantizada. . . . .	31
Figura 35 – A Lei da Radiação de Planck. . . . .	33
Figura 36 – Albert Einstein - Prêmio Nobel de Física de 1921, por suas contribuições à física teórica e, especialmente, por sua descoberta da lei do efeito fotoelétrico, que foi fundamental no estabelecimento da teoria quântica. . . . .	34
Figura 37 – Einstein - O efeito fotoelétrico, a emissão de elétrons por um material, geralmente metálico, quando exposto a uma radiação eletromagnética (como a luz) de frequência suficientemente alta, que depende do material, causa a placa perder elétrons. . . . .	35
Figura 38 – Ernest Rutherford - O pai da física nuclear: a desintegração dos elementos e a química das substâncias radioativas. . . . .	36
Figura 39 – Niels Bohr - Contribuiu decisivamente para a compreensão da estrutura atômica e da Física Quântica. . . . .	37
Figura 40 – Equação de Schrödinger dependente do tempo. . . . .	38
Figura 41 – Thomas Young - Conhecido pela experiência da dupla fenda, que em 1802 possibilitou a determinação do carácter ondulatório da luz.	58
Figura 42 – Philipp Lenard - A energia dos elétrons emitidos era independente da intensidade da luz. . . . .	59
Figura 43 – Robert Bunsen - Os padrões de luz, reconhecidos com faixas de cores diferentes . . . . .	60
Figura 44 – Louis Broglie - A natureza ondulatória dos elétrons. . . . .	61
Figura 45 – Componentes de um campo de Baseball. . . . .	62
Figura 46 – Um campo de Baseball - a posição dos jogadores. . . . .	63
Figura 47 – A dualidade onda-partícula é uma característica fundamental da mecânica quântica. . . . .	65
Figura 48 – John Wheeler - Em 1970, o experimento da escolha retardada. . . . .	66
Figura 49 – John Wheeler com Einstein - . . . . .	66

Figura 50 – Novos experimentos exploram a contínua transição de fótons agindo como partículas ou como ondas. . . . .	68
Figura 51 – Tanzilli - Entre os dois extremos, os estados que surgem da interferência. . . . .	69
Figura 52 – Peter Shadbolt - Substituindo o interruptor clássico por um bit quântico, que é um segundo fóton no experimento. . . . .	69
Figura 53 – Seth Lloyd - O fenômeno da "procrastinação quântica". . . . .	71
Figura 54 – Richard Feynman - A formulação de <b>Feynman</b> da mecânica quântica ou formulação de integrais de caminho da mecânica quântica. . . . .	71
Figura 55 – Estes são apenas três dos caminhos que contribuem para amplitude quântica de uma partícula movendo-se do ponto A em tempo $t_0$ para o ponto B em $t_1$ . . . . .	72
Figura 56 – Paul Dirac - A formulação da integral de caminho estendida para o método lagrangeano na mecânica quântica. . . . .	73
Figura 57 – Erwin Schrödinger - O modo esquisito de visualizar o comportamento quântico. . . . .	74
Figura 58 – Marlan Scully - O experimento do apagador quântico, concebido juntamente com Kai Druhl. . . . .	75
Figura 59 – Kai Druhl - O experimento do apagador quântico, concebido juntamente com <b>Marlan Scully</b> . . . . .	75
Figura 60 – Heisenberg em 1933 - O princípio da incerteza da mecânica quântica. . . . .	77
Figura 61 – Niels Bohr em 1922 - O modelo de átomo nos quais elétrons eram vistos como orbitando seu núcleo. . . . .	78
Figura 62 – Laplace - O estado presente do universo como o efeito do seu passado e a causa do seu futuro ... . . . .	79
Figura 63 – David Bohm - Converteu o experimento ERP mental inicial em algo próximo a um experimento viável. . . . .	81
Figura 64 – Albert Einstein em 1947 - Juntamente com Podolsky e Rose imaginaram o experimento ERP. . . . .	82
Figura 65 – Boris Podolsky - Juntamente com Einstein e Rose imaginaram o experimento ERP. . . . .	82
Figura 66 – Nathan Rose - A estrutura da molécula de hidrogênio, e juntamente com Einstein e Podolsky imaginou o experimento ERP. . . . .	83
Figura 67 – O experimento que comprovou com imagens, o efeito quântico conhecido como emaranhamento/entrelaçamento quântico. Múltiplas partículas estão ligadas entre si de uma forma tal que a medição do estado quântico de uma partícula determina os possíveis estados quânticos das outras partículas. . . . .	84
Figura 68 – Alain Aspect em Tel-Aviv University aos 70 anos - Em 1982, ele descobriu que as <i>desigualdades de Bell</i> eram violadas. . . . .	87
Figura 69 – Hugh Everett - A interpretação da mecânica quântica que propõe a existência de múltiplos "universos paralelos". . . . .	88
Figura 70 – Bryce DeWitt - Quem desenvolveu algumas das ideias presentes no trabalho original de <b>Hugh Everett</b> . . . . .	89
Figura 71 – John Bell - Concluiu que nenhuma teoria de variáveis locais ocultas poderia ser válida no contexto da mecânica quântica. . . . .	90
Figura 72 – John von Neumann - A proposta da não-existência de variáveis ocultas . . . . .	91
Figura 73 – Grete Hermann - O trabalho precursor para a álgebra computacional. . . . .	92
Figura 74 – John Clauser - A prova da violação das desigualdades de John Bell. . . . .	93

Figura 75 – John Archibald Wheeler - Físico estadunidense, um dos últimos colaboradores de Einstein. . . . .	94
Figura 76 – Experimento da Dupla Fenda com Projéteis - (a) Esquema do experimento de fenda dupla com projéteis. (b) Situação experimental e distribuições de probabilidades obtidas quando uma das fendas é fechada. (c) Situação experimental e distribuição de probabilidade obtida quando as duas fendas estão abertas. . . . .	100
Figura 77 – Esquema do experimento de fenda dupla com ondas. As intensidades $I_1$ e $I_2$ correspondem às situações onde apenas os buracos 1 ou 2 estão abertos, respectivamente. Já a intensidade $I_{12}$ corresponde à situação em que os dois buracos estão abertos simultaneamente. . . . .	102
Figura 78 – Thomas Young - Físico, a experiência da dupla fenda com ondas de luz. . . . .	103
Figura 79 – Experimento da Dupla Fenda - a luz visível se difracta através de duas fendas. . . . .	104
Figura 80 – Esquema do experimento de fenda dupla com elétrons. . . . .	106
Figura 81 – Montagem experimental e painel de controle do experimento virtual de interferência por uma fenda dupla. . . . .	107
Figura 82 – Claus Jönsson - Em 1961, a primeira experiência de interferência de elétrons por fenda dupla. . . . .	108
Figura 83 – Molécula de carbono 60 - A interferência de fenda dupla com moléculas de $C_{60}$ . . . . .	109
Figura 84 – Markus Arndt - Em 1999, o físico que verificou a interferência de fenda dupla com moléculas de carbono $C_{60}$ . . . . .	109
Figura 85 – Polarização de fótons - Filtro A. . . . .	111
Figura 86 – Polarização de fótons - Filtro A. . . . .	111
Figura 87 – Polarização de fótons inicial em A - Filtro A. . . . .	112
Figura 88 – Polarização de fótons - Filtros A e C. . . . .	112
Figura 89 – Polarização de fótons - Filtros A, B e C. . . . .	113
Figura 90 – Polarização de fótons - Filtros A, B e C. . . . .	113
Figura 91 – Um medição - É uma projeção sobre a base, onde $a = \alpha$ e $b = \beta$ . . . . .	114
Figura 92 – Denominações em determinados grupos. . . . .	125
Figura 93 – Simetrias de um quadrado. . . . .	126
Figura 94 – Tabela de Cayley das simetrias de um quadrado. . . . .	126
Figura 95 – Métrica de Manhattan versus Distância Euclidiana. . . . .	134
Figura 96 – Augustin Cauchy - Matemático francês que se destacou no estudo das sequências e séries numéricas no século XVIII. . . . .	139
Figura 97 – O espaço vetorial $\mathbb{R}^n$ vem com uma base padrão (base canônica). . . . .	141
Figura 98 – David Hilbert - Criação dos espaços que levam seu nome, durante seus trabalhos em análise sobre equações integrais. . . . .	142
Figura 99 – Leopold Kronecker - Uma das suas frases mais famosas é: Deus criou os inteiros; todo o resto é trabalho do homem. . . . .	143
Figura 100 – Stefan Banach - o criador da moderna Análise Funcional, que trata do estudo de espaços de funções. . . . .	146
Figura 101 – John von Neumann - Modelou a mecânica quântica em um espaço de Hilbert. . . . .	147
Figura 102 – Volterra - Quem criou a palavra "funcional" no Cálculo das Variações. . . . .	147
Figura 103 – Em um espaço de Hilbert $n$ -dimensional, como podemos ver o produto externo de estados. . . . .	148
Figura 104 – Propriedades numa base ortonormal de um espaço de Hilbert. . . . .	149

Figura 105	– A esfera de Bloch mostra uma representação de um <i>qubit</i> , o bloco de construção fundamental de computadores quânticos, representado na superfície de uma esfera de raio 1. . . . .	158
Figura 106	– Charles Hermite - Foi o primeiro a utilizar a terminologia "Matrizes Ortogonais" e criador das matrizes hermitianas. . . . .	165
Figura 107	– W. R. Hamilton - Operador Hamiltoniano, Autofunções e Autovalores. . . . .	167
Figura 108	– Operador Hamiltoniano, Autofunções e Autovalores. . . . .	170
Figura 109	– Propriedades associativa e distributiva de tensores. . . . .	173
Figura 110	– Propriedades algébricas para matrizes-tensores em espaço de matrizes. . . . .	174
Figura 111	– David Deutsch - O Universal Quantum Computer e seu simples algoritmo quântico. . . . .	180
Figura 112	– Peter Zoller - O trabalho pioneiro sobre computador quântico. . . . .	181
Figura 113	– Ignacio Cirac - A pesquisa para armazenar <i>qubits</i> e executar cálculos quânticos. . . . .	182
Figura 114	– Peter Shor - Aos 35 anos, quando criou o algoritmo quântico para fatorar inteiros. . . . .	182
Figura 115	– Produto Tensorial entre P e Q. . . . .	188
Figura 116	– Produto Tensorial entre P e Q. . . . .	189
Figura 117	– A diferença entre um bit e um qubit. . . . .	190
Figura 118	– Ilustração do Princípio da Superposição. . . . .	191
Figura 119	– Um computador quântico de 3 qubits. . . . .	192
Figura 120	– Tabela Qubits versus Bits: atualmente, já estamos em 79 qubits do computador quântico IonQ. . . . .	193
Figura 121	– Superposição, Interferência e a dualidade partícula-onda. . . . .	194
Figura 122	– Otto Stern - um físico estadunidense nascido na Alemanha, laureado com o Nobel de Física de 1943. . . . .	195
Figura 123	– Walther Gerlach - um físico alemão, co-descobridor do experimento que descobriu os spins de Stern-Gerlach. . . . .	196
Figura 124	– Um computador quântico líquido. . . . .	196
Figura 125	– Spins alinhados. . . . .	197
Figura 126	– Spins alterados e de volta à configuração original. . . . .	197
Figura 127	– A placa acima, no Instituto de Física de Frankfurt (Alemanha), comemora o experimento de Stern (à esquerda) e Gerlach que levou à descoberta do 'spin' (foto: Wikimedia Commons/Peng - CC 3.0 BY-SA). . . . .	198
Figura 128	– O esquema genérico para um computador quântico de $n$ qubits. . . . .	199
Figura 129	– John von Neumann - A modelagem algébrica da teoria quântica com os espaços de Hilbert. . . . .	203
Figura 130	– John von Neumann - The Mathematical Foundations of Quantum Mechanics. . . . .	205
Figura 131	– Karl Popper - considerado um dos maiores filósofos da ciência do século 20, pensador sobre a lógica da pesquisa científica. . . . .	208
Figura 132	– Paul Benioff - Pioneiro na pesquisa em teoria da informação quântica que demonstrou a possibilidade teórica de computadores quânticos. . . . .	209
Figura 133	– Richard Feynman - O pioneiro na eletrodinâmica quântica e na área de computação quântica, introduzindo o conceito de nanotecnologia. . . . .	211
Figura 134	– David Albert - descreveu uma medida na mecânica quântica, baseada num autômato. . . . .	213

Figura 135–Visão comparativa entre um computador clássico e um quântico. . . . .	217
Figura 136–Visão comparativa entre o bit clássico e um bit quântico (qubit). . . . .	220
Figura 137–Esfera de Bloch. . . . .	221
Figura 138–Dois estado quânticos genéricos $ \psi\rangle$ e $ \phi\rangle$ . . . . .	222
Figura 139–Produto tensorial de dois estados quânticos genéricos $ \psi\rangle$ e $ \phi\rangle$ . . . . .	222
Figura 140–Um vetor de estado quântico genérico $ \psi\rangle$ . . . . .	222
Figura 141–Um produto tensorial de estados genéricos $ \psi\rangle$ e $ \phi\rangle$ . . . . .	222
Figura 142–Linearidade quando apenas um qubit de dois qubits é medido. . . . .	223
Figura 143–Quando a medida de dois qubits não é feita separada. . . . .	223
Figura 144–A medida do estado genérico do sistema quântico corresponde ao produto tensorial dos estados genéricos individuais de cada qubit. . . . .	224
Figura 145–Histórico das portas lógicas clássicas. . . . .	224
Figura 146–Os valores lógicos na Álgebra Booleana. . . . .	225
Figura 147–Os valores lógicos na Álgebra Booleana. . . . .	225
Figura 148–Os valores lógicos na Álgebra Booleana. . . . .	226
Figura 149–Porta NOT da lógica binária. . . . .	227
Figura 150–Porta X quântica (CNOT quântica). . . . .	227
Figura 151–Porta $U$ unitária. . . . .	227
Figura 152–Porta $U$ unitária. . . . .	228
Figura 153–Porta $Z$ . . . . .	228
Figura 154–Jacques Hadamard - Teve uma de suas matrizes aplicada para definir uma porta quântica. . . . .	229
Figura 155–Porta $H$ : Hadamard. . . . .	229
Figura 156–Wolfgang Pauli - Teoria do Spin e o princípio de exclusão em 1925. . . . .	230
Figura 157–Portas de 2 bits da lógica clássica. . . . .	230
Figura 158–As portas Y (Pauli-Y ) as portas de inversão. As portas S (Fase) e T ( $\pi/8$ ). . . . .	231
Figura 159–Porta CNOT de 2 qubits da lógica quântica. . . . .	231
Figura 160–Tabela do operador CNOT aplicada aos estados fundamentais de um sistema de 2 qubits da lógica quântica. . . . .	232
Figura 161–Porta TROCA construída a partir de porta CNOT, que faz a troca dos estados entre os dois <i>qubits</i> . . . . .	232
Figura 162–Porta U controlada para 2 qubits. . . . .	233
Figura 163–Circuito para medir o valor de um qubit. . . . .	233
Figura 164–Circuito de um somador quântico. . . . .	235
Figura 165–Circuito quântico de teleporte (ISAILOVIC, 2004). . . . .	236
Figura 166–Estado do qubit teleportado após a realização da medida nos qubits originais. . . . .	237
Figura 167–Teleporte quântico é de fato possível. . . . .	238
Figura 168–Proposta de Arquitetura de Computador Quântico (OSKIN; CHONG; CHUANG, 2002). . . . .	239
Figura 169–Perspectivas da Computação Quântica (HUGHES R., 2010). . . . .	242
Figura 170–Dois tipos de computadores quânticos - Aplicações, generalidade e poder computacional. . . . .	246
Figura 171–Isaac Chuang segura frasco com solução com as moléculas que funcionaram como um computador quântico; à dir., estrutura da molécula. As operações que permitiram fatorar o número 15 foram realizadas pelos átomos numerados de 1 a 7. . . . .	247
Figura 172–Esquema de funcionamento do D-Wave-2. . . . .	248
Figura 173–Ionq-chip - O IonQ funciona com a captura de íons de itérbio num campo eletromagnético. . . . .	249

Figura 174–Peter Shor - O algoritmo quântico de fatoração de números primos grandes. . . . .	255
Figura 175–A fatoração de números primos. . . . .	256
Figura 176–Lov Grover - O inventor do algoritmo de busca quântico em uma base de dados. . . . .	260
Figura 177–Circuito quântico para o algoritmo de Grover. . . . .	262
Figura 178–A matriz D do circuito quântico do algoritmo de Grover. . . . .	262
Figura 179–Função constante ou balanceada ? . . . . .	263
Figura 180–Exemplo de função constante ou balanceada. . . . .	263
Figura 181–Circuito quântico para o algoritmo de Deutsch. . . . .	263
Figura 182–Relações entre classes de complexidade clássicas e quânticas. . . . .	264
Figura 183–Algoritmos criptográficos em geral. . . . .	267
Figura 184–Algoritmos criptográficos - a cifra <i>One Time Pad</i> . . . . .	268
Figura 185–Diferentes planos de polarização de um fóton. . . . .	269
Figura 186–Um exemplo de filtro polaroide. . . . .	269
Figura 187–Exemplo de polarizações referentes aos bits 0 e 1, no protocolo BB84. . . . .	270
Figura 188–Explicação do funcionamento do protocolo BB84. . . . .	270
Figura 189–Passos do protocolo até a obtenção da chave $k$ . . . . .	271
Figura 190–Explicando os passos do BB84. . . . .	271
Figura 191–Stephen Wiesner - Aos 28 anos, a ideia em 1970 que norteou a criptografia quântica por Charles Bennett. . . . .	273
Figura 192–Charles Henry Bennett é um físico, criptógrafo e cientista da computação estadunidense. É um dos descobridores do teletransporte quântico. . . . .	274
Figura 193–Claude Shannon em 1963 - Um matemático, engenheiro eletrônico e criptógrafo estadunidense, conhecido como o pai da "teoria da informação". . . . .	276
Figura 194–Norbert Wiener - Sobre a entropia da informação: o grau de organização ou desorganização em um sistema de informação. . . . .	276
Figura 195–Polarizações de fótons na comunicação de Alice e Bob. . . . .	278
Figura 196–Gilles Brassard - Juntamente com Charles Bennett desenvolveu um sistema prático de criptografia quântica, baseado no princípio da incerteza, conhecido como BB84. . . . .	279
Figura 197–Criptografia Quântica - A comunicação quântica entre Alice e Bob. . . . .	280
Figura 198–Criptografia Quântica BB84 - A comunicação quântica entre Alice e Bob. . . . .	281
Figura 199–Criptografia Quântica BB84 - Passos de execução do protocolo BB84 no caso ideal. . . . .	281
Figura 200–Criptografia Quântica BB84 - Passos de execução do protocolo BB84 na presença de Eva. . . . .	282
Figura 201–Coordenadas esféricas - Indicando a direção das polarizações. . . . .	283
Figura 202–Representação das bases A e B. O eixo z não está desenhado pois temos polarizações pertencentes ao plano xy. . . . .	284
Figura 203–As cinco primeiras linhas correspondem à transmissão quântica. As outras cinco, à discussão pública entre Alice e Bob. A última linha representa a chave compartilhada por eles. . . . .	285
Figura 204–John A. Smolin - Juntamente com Charles H. Bennett, construiu a primeira demonstração de criptografia quântica em 1989. . . . .	286
Figura 205–William Wothers - Teoria do emaranhamento quântico e a descoberta do teletransporte quântico. . . . .	287

Figura 206–Benjamim Schumacher - Descobriu uma maneira de interpretar estados quânticos como informação. . . . .	287
Figura 207–David DiVincenzo - o computador quântico baseado em spins de eletrons em 1997. . . . .	288
Figura 208–Daniel Loss - O computador quântico Loss-DiVincenzo em 1997, baseado em spins de eletrons. . . . .	289
Figura 209–Ilustração do protocolo B92. . . . .	290
Figura 210–Criptografia Quântica para controle de acesso à Big Data. . . . .	292
Figura 211–Tipos de criptografia viáveis de ser construídas. . . . .	295
Figura 212–Como no emaranhamento quântico ... . . . .	299

# Lista de tabelas

Tabela 1 – Pontos especiais sobre a Esfera de Bloch . . . . .	220
---	-----





# Sumário

<b>Prefácio</b> . . . . .	<b>xix</b>
<b>Apresentação</b> . . . . .	<b>xxi</b>
<b>I A Física</b> . . . . .	<b>xxv</b>
<b>1 Da Física Clássica ao Início da Física Quântica</b> . . . . .	<b>1</b>
1.1 Galileu Galilei . . . . .	1
1.2 Huygens - 1690 . . . . .	2
1.3 Newton - 1704 . . . . .	3
1.4 Ampère . . . . .	3
1.5 Thomas Young e Jean Fresnel . . . . .	5
1.6 Charles - 1787 . . . . .	6
1.7 Orsted - 1806 . . . . .	6
1.8 Carnot - 1824 . . . . .	8
1.9 Faraday - 1831 . . . . .	9
1.10 Balmer - 1848 . . . . .	9
1.11 Joule - 1849 . . . . .	10
1.12 Clausius - 1850 e 1865 . . . . .	10
1.13 Kelvin . . . . .	12
1.14 Gustav Kirchhoff - 1859 . . . . .	13
1.15 Maxwell - 1864 e 1873 . . . . .	14
1.16 John Strutt (Lord Rayleigh) - 1877 e 1889 . . . . .	14
1.17 Os resultados de Stefan-Boltzmann - 1879 . . . . .	15
1.18 Rydberg e os comprimentos de onda de fótons - 1888 . . . . .	17
1.19 Wilhelm Wien - 1893 . . . . .	18
1.20 JJ Thomson -1897 . . . . .	19
1.21 Lummer e Pringshein, 1899, as primeiras medidas de um corpo negro . . . . .	21
1.22 O início da mecânica quântica . . . . .	21
1.23 Rayleigh-Jeans e a distribuição espectral de um corpo negro . . . . .	23
1.24 Bibliografia e Fonte de Consulta . . . . .	24
1.25 Referências e Leitura Recomendada . . . . .	26
<b>2 O Século da Física Quântica</b> . . . . .	<b>29</b>
2.1 A emissão de radiação do corpo negro . . . . .	29
2.2 Marx Planck - 1900 . . . . .	30
2.2.1 Planck resolveu o problema . . . . .	32
2.2.2 A ideia da quântica: energia existente apenas em certos níveis . . . . .	32
2.3 Einstein e o efeito fotoelétrico - 1905 . . . . .	33
2.4 O modelo atômico de Rutherford - 1911 . . . . .	35
2.5 Niels Bohr: um novo modelo de átomo adotando uma abordagem quântica - 1913 . . . . .	35
2.6 A contribuição de Schrödinger - 1925 . . . . .	37
2.7 Princípio da Incerteza de Heisenberg - 1927 . . . . .	39
2.8 Bibliografia e Fonte de Consulta . . . . .	41
2.9 Referências e Leitura Recomendada . . . . .	42
<b>3 A Revolução Quântica</b> . . . . .	<b>45</b>
3.1 A revolução quântica . . . . .	45
3.2 Cinco conceitos para se começar a entender a mecânica quântica . . . . .	46

3.2.1	As partículas são ondas, e vice-versa	47
3.2.2	Tudo o que podemos saber são probabilidades	47
3.2.3	O uso da probabilidade - o <i>sim</i> , o <i>não</i> e o <i>talvez</i>	48
3.2.4	As correlações quânticas não são locais	48
3.2.5	A Física quântica é real	49
3.3	A revolução da Teoria Quântica	50
3.4	Bibliografia e Fonte de Consulta	54
3.5	Referências e Leitura Recomendada	54
<b>4</b>	<b>A Base Experimental da Mecânica Quântica</b>	<b>55</b>
4.1	A luz é onda ou partícula?	57
4.2	Einstein e o efeito fotoelétrico	59
4.3	A matéria é onda ou partícula? -1924	60
4.4	Decisões divididas: Experimentos com divisores de feixes	61
4.4.1	O Campo	62
4.4.2	O que é Baseball - uma breve explicação	62
4.4.3	O experimento com divisores de feixes	63
4.5	Como os fótons sabem ?	64
4.6	O Comportamento do fóton	67
4.7	Ondas de probabilidade e observações: Um exemplo humano	72
4.8	Você não é ninguém antes de ser observado	72
4.9	O gato de Schrödinger	73
4.10	Apagadores quânticos	74
4.11	O princípio da incerteza	76
4.12	Emaranhamento e o experimento EPR de Einstein, Podolsky e Rosen	80
4.12.1	Exemplo clássico de Emaranhamento Quântico	85
4.13	EPR, o Estado Emaranhado e as Variáveis Ocultas	85
4.13.1	A Interpretação de Copenhagen	86
4.13.2	A Interpretação dos Muitos Mundos	86
4.14	O Teorema de Bell	88
4.15	O primeiro round	93
4.16	A incerteza por princípio	94
4.17	Bibliografia e Fonte de Consulta	95
4.18	Referências e Leitura Recomendada	96
<b>5</b>	<b>Os Experimentos da Dupla-Fenda</b>	<b>99</b>
5.1	Um experiência com projéteis	99
5.2	Uma experiência com ondas de água	101
5.3	Uma experiência com ondas de luz	103
5.4	Uma experiência com ondas de um feixe eletrônico	103
5.5	Uma experiência com elétrons	105
5.5.1	Interferência de ondas de elétrons	106
5.6	Experimento da Dupla-Fenda Virtual	107
5.6.1	A experiência com elétrons	107
5.7	Polarização de Fótons	110
5.7.1	O experimento	111
5.7.2	A explicação	112
5.8	Princípios da Incerteza e da Complementaridade	115
5.9	Bibliografia e Fonte de Consulta	116
5.10	Referências e Leitura Recomendada	117

<b>II</b>	<b>A Matemática</b>	<b>119</b>
<b>6</b>	<b>A Base Matemática Algébrica</b>	<b>121</b>
6.1	Análise Funcional	121
6.2	Teoria dos Grupos algébricos	123
6.3	Grupo e Simetrias	125
6.4	Teoria dos Anéis algébricos	127
6.5	John von Neumann e a Teoria de Álgebra de Operadores	128
6.6	Teoria de anéis de polinômios	130
6.7	Polinômios de Hermite	131
6.8	Corpos Algébricos	131
6.9	Conceituando um Espaço matemático	133
6.10	Conceituando um Espaço Métrico	133
6.11	O conceito de Espaço Vetorial	134
6.12	Norma matemática	135
6.13	Métrica e topologia induzida	136
6.14	Conceituando um Espaço Topológico	136
6.15	Produto interno	137
6.16	Norma a partir de um produto interno	138
6.17	Espaços completos	138
6.18	Bibliografia e Fonte de Consulta	140
6.19	Para saber mais - Leitura Recomendada	140
<b>7</b>	<b>Espaços de Hilbert</b>	<b>141</b>
7.1	Espaços de Hilbert	141
7.2	Base Canônica	142
7.3	Espaço vetorial com produto interno	144
7.4	Espaço vetorial, Produto interno e Norma	144
7.5	Definições do Espaço de Hilbert	145
7.6	Espaço de Hilbert conjugado	148
7.7	Ortogonalidade e Ortonormalidade	148
7.8	Operadores lineares	149
	7.8.1 Operadores e suas propriedades	150
	7.8.2 Operadores num espaço de Hilbert	150
7.9	Bibliografia e Fonte de Consulta	152
7.10	Referências e Leitura Recomendada	153
<b>8</b>	<b>Espaços de Hilbert e a Teoria Quântica</b>	<b>155</b>
8.1	Espaços Vetorial nos Números Complexos	156
8.2	Bases e Dimensão	157
8.3	Postulados da mecânica quântica	160
8.4	Operadores na mecânica quântica	162
8.5	Problema de autovalores e autovetores	166
8.6	Operador Hamiltoniano	167
8.7	Autovalores, Autovetores e Representação Espectral	170
8.8	Produto Tensorial	171
8.9	Bibliografia e Fonte de Consulta	175
8.10	Para saber mais - Leitura Recomendada	175
<b>III</b>	<b>A Computação Quântica</b>	<b>177</b>
<b>9</b>	<b>Da Mecânica Quântica à Computação Quântica</b>	<b>179</b>
9.1	Além da tese de Church-Turing	179
9.2	A necessidade da Computação Quântica	181

9.3	O que é Computação Quântica?	183
9.4	O qubit e suas propriedades	184
9.4.1	Estados quânticos	188
9.4.2	Observáveis e medições	189
9.5	Os Fundamentos da Computação Quântica	189
9.5.1	Diferenciando estados quânticos	189
9.5.2	O Princípio da Superposição	190
9.5.3	Implementando qubits	194
9.5.4	Caracterizando o Computador Universal Quântico	199
9.6	Bibliografia e Fonte de Consulta	199
9.7	Para saber mais	200
<b>10</b>	<b>Uma Introdução à Computação Quântica</b>	<b>203</b>
10.1	A contribuição de John von Neumann à Teoria Quântica	204
10.2	Máquina de computação e o princípio de Church-Turing	204
10.3	Os pioneiros do computador quântico	208
10.4	Os princípios do computador quântico	214
10.5	A incerteza por princípio	215
10.6	Bits e quBits	216
10.7	O uso da probabilidade	218
10.8	Entendendo estados quânticos com dois qubits	218
10.9	Portas lógicas clássicas	224
10.10	Portas lógicas quânticas	224
10.11	Portas de 1 qubit	226
10.11.1	Porta NOT quântica	226
10.11.2	Porta CNOT quântica	227
10.11.3	Porta U unitária	227
10.11.4	Porta Hadamard	228
10.11.5	As portas de Pauli	228
10.12	Portas de n qubits e Operações Quânticas	230
10.12.1	Porta CNOT quântica : NOT controlada	231
10.12.2	Porta U controlada para dois qubits	232
10.12.3	Medindo um qubit	232
10.13	Computação reversível	233
10.14	Juntando as partes	234
10.15	Teleporte Quântico	235
10.16	Construindo a Arquitetura	237
10.17	Computadores Quânticos podem funcionar	240
10.18	Computador quântico x Computador digital	242
10.19	O computador e a computação quântica	244
10.20	Simulação de sistemas quânticos	245
10.21	Dois tipos de computadores quânticos	245
10.22	Computadores quânticos - outros marcos importantes	245
10.23	Conheça o IonQ	249
10.24	História, Startups e Perspectivas	250
10.25	Bibliografia e Fonte de Consulta	251
10.26	Para saber mais ... Leitura Recomendada	252
<b>11</b>	<b>Algoritmos e Computação Quântica</b>	<b>253</b>
11.1	Um Algoritmo Quântico em geral	253
11.2	Preparando para entender o algoritmo de Shor - 1994	254
11.2.1	Algoritmo de Fatoração de Shor	254
11.2.2	Da teoria dos números ...	255
11.2.3	Visão geral do algoritmo de Shor	256

11.3	Algoritmo Quântico de Lov Grover - 1996	259
11.4	O problema de Deutsch-Jozsa - 1992	262
11.5	Para saber mais sobre Shor	265
11.6	Para saber mais sobre Grover	265
11.7	Para saber mais sobre Deutsch	266
11.8	Para saber mais ... Teoria da Complexidade Quântica	266
<b>12</b>	<b>Criptografia Quântica</b>	<b>267</b>
12.1	Algoritmos criptográficos	267
12.2	Princípios da mecânica quântica - a polarização de fótons	268
12.3	Um protocolo de bases conjugadas - BB84	269
12.4	A presença de um intruso	270
12.5	Histórias de Stephen Wiesner ...	272
12.6	A primeira ideia de um sistema de criptografia quântico	274
12.7	Entropia da Informação	275
12.8	A Criptografia quântica de Bennett	277
12.9	Um sistema prático de criptografia quântica	277
12.10	O Protocolo BB84	278
12.11	O Protocolo E91	288
12.12	Protocolo B92	289
12.13	Protocolo BBM92	290
12.14	Oblivious Transfer Protocol - Transferência Inconsciente	290
12.15	Criptografia quântica para acesso em Big Data	291
12.16	Six-State Protocol	291
12.17	Tecnologias para a Criptografia Quântica	292
12.18	Quantum money - O futuro	293
12.19	Desafios na Comunicação com Criptografia Quântica	294
12.20	Tipos de criptografia quântica	294
12.21	Recomendações	294
12.22	Bibliografia e Fonte de Consulta	295
12.23	Referências e Leitura Recomendada	297
<b>Posfácio</b>		<b>299</b>
<b>Referências</b>		<b>301</b>



# Prefácio

Podemos dizer que dentre as atividades intelectuais humanas, as principais são a ciência e a filosofia. Dentre estas, as consideradas mais importantes para o mundo atual são a matemática, a física, a ciência da computação e a filosofia. Mas a natureza da computação como ciência, mas precisamente, a computação quântica tem como raiz e foco, vinculados à história da física quântica e à filosofia.

Assim é a teoria quântica. Postulados, conceitos, princípios e teoremas estão em um contexto histórico em que o homem, em seu desejo de aprender foi estabelecendo as bases da computação quântica durante a construção de sua trajetória rumo à sociedade da informação.

Durante sua evolução histórica a computação quântica vem passando de níveis, de total complexidade para maior utilização nas suas áreas de domínio. Ou seja, desde as primeiras ideias de **Planck**, **Einstein**, **Niels Bohr**, **Schrödinger**, os princípios como o de **Heisenberg**, aos teoremas da mecânica quântica, ou mesmo aos operadores como os *hamiltonianos* da mecânica quântica, que cada problema e solução estão ligados à história que deve ser conceitualmente compreendida em relação ao tempo e espaço.

Não temos como entender a computabilidade quântica sem a sua perspectiva histórica. Assim, liga-se a história ao tempo-espaço dos problemas e a história liga **Hilbert** com **John von Neumann**, e mais **Planck**, **Einstein**, **Heisenberg**, **Dirac**, **Schrödinger**, **Niels Bohr** e outros, mostrando como as principais teorias da física moderna foram criadas.

A perspectiva histórica também é importante para compreender como **Einstein** chegou, não só à teoria da relatividade, mas também ao mundo quântico, e a sua busca pela teoria geral do universo, ou como **Heisenberg** chegou ao *princípio da incerteza* buscando pela posição do elétron. Como todos se relacionam? Se relacionam por meio da transformação histórica de conceitos que vão se juntando como um enorme quebra-cabeça. Só a história pode mostrar que as teorias que estudamos hoje foi gerada por um processo construído no tempo da jornada da humanidade. Uma jornada de milhares de anos de teorias obtidas pela ciência e experimento. Assim, surgiu a mecânica quântica, que aplicada à ciência da computação, vem causando o surgimento dos computadores quânticos.

A história, na verdade, é quem molda as teorias. A relatividade de **Einstein** nunca foi sua principal teoria. Um dos matemáticos da teoria quântica era **von Neumann** que propôs o modelo da computação determinística. Vejam que paradoxo! Um dos cientistas da teoria quântica, nada determinística, propõe um modelo de arquitetura para o computador clássico como uma máquina de estados determinística.



Podemos dizer que a ciência é investigativa, mas grande parte nasce da criatividade, da intuição e da interatividade humana, ou seja, do processo histórico. Portanto, há que se diferenciar entre o modelo investigativo da Física, entre o modelo teórico e o experimental. Sendo a Física quântica uma ciência com base em postulados toda validação de resultados dessa Física como modelo investigativo teórico, é corroborado por ela mesma como ciência experimental. Desta forma podemos dizer que o contexto histórico é fundamental para a compreensão do seu conteúdo. Certamente, a mecânica quântica atingiu, hoje, uma importância crucial para a construção do computador quântico.

A computação quântica tem uma teia de relações com várias áreas do conhecimento. As relações da computação quântica e outras ciências já podem ser observadas desde a década de 40, no século XX. Assim forma-se a base para a um livro de suma importância para um primeiro aprendizado. Um livro que é fundamental para a compreensão, pelo leitor, de como surgiram as ideias quânticas. Antes de deduzir e demonstrar os teoremas principais ou mais elaborados da matemática, é importante mostrar ao leitor as bases a partir das quais foram enunciados os problemas e como foi conduzida sua solução com o alicerce matemático existente. Mas o livro não para por aí. Trata-se de uma leitura que nos transporta à visão de problemas e soluções quânticas em seu tempo; na sua origem; ou na sua fonte. Organizado, preferencialmente numa linha temporal, o livro aborda os diversos problemas/fenômenos de uma maneira interdependente, mostrando que os conceitos fundamentais se mantêm e, se aplicam às descobertas físicas cada vez mais complexas.

Evitando a grande dificuldade de expor e demonstrar as modernas teorias quânticas, o livro compensa pela facilidade de expor as ideias sobre elas e como foram elaboradas, questionadas e resolvidas. Torna-se mais fácil entender e mais evidente de se constatar as relações conceituais do homem e sua obra no contexto temporal da evolução desta ciência. É como compreender de que maneira a computação quântica vai se revelando a si mesma e por si mesma. É a história permitindo a formação do homem acostumado à discussão científica e ao pensamento matemático na ciência da computação. Resta-me apenas desejar uma boa leitura.

Florianópolis, Junho de 2019

João Cândido Dovicchi  
Departamento de Informática e Estatística da UFSC

# Apresentação

Este é o terceiro volume da série de livros intitulada **Pensamento Matemático @ Ciência da Computação**, disponibilizado em sua primeira forma de publicação, no Repositório Institucional da UFSC, como resultado do projeto de extensão Sigpex 2016.11146, INE/UFSC.

A computação quântica é a ciência que estuda as aplicações das teorias e propriedades da mecânica quântica na ciência da computação. Dessa forma seu principal foco é o desenvolvimento do computador quântico. Embora, na comunidade acadêmica brasileira já se encontre, há muito tempo, diversos trabalhos direcionados à computação quântica, os trabalhos no INE (Departamento de Informática e Estatística da UFSC) e no PPGCC/UFSC, somente agora começam a despertar para o futuro da ciência da computação. Louva-se a iniciativa pessoal do Prof. **João Cândido Dovicchi**, quando ainda no seu trabalho no dia-a-dia do departamento, não chegou a ser amplamente difundida.

Da parte dos autores deste trabalho, a publicação dos dois primeiros volumes da série **Pensamento Matemático @ Ciência da Computação** - "*Dos Primórdios da Matemática aos Sistemas Formais da Ciência da Computação*" (Volume I) e "*Da Computabilidade Formal às Máquinas Programáveis*" (Volume II) - criou a oportunidade de organizarmos este terceiro volume, no sentido de reunir num único lugar, a história fascinante da Teoria Quântica na primeira parte deste volume, organizando os fundamentos da matemática algébrica na segunda parte, e abordando na sua terceira parte, a computação quântica, numa visão dos fundamentos de um sistema quântico computacional. Esta terceira parte traz à tona, os conceitos relevantes que norteiam a construção do computador quântico. Paralelamente a este trabalho, a Profa. **Jerusa Marchi** (INE/UFSC) vem evoluindo, junto com o grupo de pesquisa do Departamento de Física da UFSC, no sentido de conhecer a área. A iniciativa do grupo da Física na UFSC é facilitada pelo conhecimento da mecânica quântica, base da computação quântica. E vem se constituindo na iniciativa mais forte no sentido da ciência da computação quântica na UFSC.

O ensino da computação quântica no INE, precisa passar por mudanças significativas, pois estamos atrasados com relação a conjuntura das instituições brasileiras constituindo a comunidade quântica. Nem mesmo aulas expositivas convencionais são predominantes no nosso meio. A proposta deste livro procura contribuir para essa mudança. Assim, damos atenção a marcos históricos no desenvolvimento quântico, como o início de aprendizagem. Além disso, a atividade de pesquisa de mestrado, a partir de agora, poderá incluir uma linha de pesquisa, mesmo teórica, como tem sido o aprendizado em outros programas de pós-graduação no Brasil, e possa ser utilizado por outros professores de forma independente do mestrado.

Nossa proposta é modesta. Este livro apresenta a história fantástica, desde a base conceitual dos experimentos reveladores da mecânica quântica até os conceitos básicos da computação quântica. Tal conteúdo não aparece, ainda, nos currículos dos cursos de ciência da computação. A intenção do material do livro é servir de apoio na aquisição do conhecimento sobre a computação quântica, quanto aos seus aspectos físicos e matemáticos (algébricos), num curso de ciência da computação. Embora trate-se de uma tem abstrato, pensamos no principal diferencial deste trabalho ser de caráter pedagógico, direcionado a um público abrangente, que não necessariamente tenha conhecimentos prévios sobre mecânica quântica. Daí, a ordem natural dos capítulos, no sentido de amenizar a dificuldade de entendimento do tema.

O trabalho dos autores consistiu num levantamento bibliográfico e reúne neste volume, uma forma mais organizada em relação ao material que está espalhado na literatura, em vários livros e na Internet, sobre o tema quântico. Este livro foi organizado como um texto de apoio aos docentes e alunos, e aborda os temas gerais com fatos históricos, experiências reveladoras, conceitos quânticos, a matemática algébrica dos sistemas quânticos e, chegando-se aos aspectos da computação quântica, no que tange à construção de um computador quântico. A escolha dos capítulos e sua apresentação são, obviamente, autorais. Os capítulos seguem uma ordem natural, no sentido de mostrarmos as raízes da computação quântica. Consequentemente, não se trata de um livro totalmente didático de Computação Quântica independente de outros bons textos disponíveis. No entanto, pode ser de apoio ao entendimento inicial do tema quântico. O principal diferencial deste trabalho é o seu caráter motivador, direcionado a um público abrangente, que não necessariamente tenha conhecimentos prévios sobre **mecânica quântica**.

Tratamos da transição da Física clássico-quântica. Nossa abordagem mostra uma área não muito simples de ser entendida, abstrata por natureza, mas colocada do ponto de vista histórico, mostra as grandes ideias e alguns dos personagens de renome como (JJ Thomson (1897), **Max Planck** (1900), **Albert Einstein** (1905), **Ernest Rutherford** (1911), **Neils Bohr** (1913), **Erwin Schrödinger** (1926), **Werner Heisenberg** (1927), **Paul Dirac** (1928), **Wolfgang Pauli** (1931), **Paul Benioff** (1980), **Richard Feynman** (1980), **Bennett** (1984), **Deutsch** (1985), **Shor** (1994), **Grover** (1996) entre outros, nos fatos mais marcantes da física, da matemática e da computação quântica.

Aqui é mostrada a iniciativa matemática de **John von Neumann**. Por essa altura, conheceu **David Hilbert**, um matemático que viria a ter grande influência no seu trabalho. **John von Neumann** dedicou-se à axiomatização da mecânica quântica em 1926, quando percebeu que um sistema quântico podia ser considerado um ponto num espaço Hilbertiano, e usou a matemática algébrica para modelar esses sistemas, utilizando-se dos espaços de **Hilbert**. E a física da mecânica quântica foi reduzida à matemática de operadores hermitianos/hamiltonianos em espaços de **Hilbert**.

Na terceira parte do livro, abordamos três capítulos, destinados a introduzir a computação quântica, do ponto de vista das portas lógicas quânticas e o último, abordando o conceito de algoritmo quântico e computação quântica. E por fim, mostrar o campo da criptografia quântica, destacando os trabalhos mais conhecidos.

A série de livros intitulada **Pensamento Matemático @ Ciência da Computação** é aberta aos que lidam com matemática, lógica e ciência da computação, a qual não seria possível de ser constituída a baixo custo, sem o *template LaTeX ABNTeX2*

para edição, sem o prefixo editorial acessível na Agência Brasileira do ISBN, sem o serviço de catalogação da BU-UFSC e o meio imediato de publicação no Repositório Institucional da UFSC.

Os autores imaginam que este trabalho proporcione às pessoas os meios de começar a entender este tema, que será mais apreciado, para os que se adaptarem à abstração dessas ciências. Desejamos assim, contribuir para que graduandos, mestrandos e professores e demais interessados possam entender e refletir sobre o futuro da ciência da computação: a computação quântica. Boa leitura.

Florianópolis, Julho de 2019

João Bosco M. Sobral  
- Departamento de Informática e Estatística da UFSC  
Renato Bobsin Machado  
- Pós-Graduação em Engenharia Elétrica e Computação da UNIOESTE-Foz do Iguaçu.



Parte I  
A Física



# Da Física Clássica ao Início da Física Quântica

Pode-se traçar a história da Física a partir do momento em que a humanidade começou a ver e analisar os fenômenos naturais de modo racional, abandonando explicações místicas ou divinas. As primeiras tentativas racionais de explicação da natureza vieram com os indianos e com os gregos antigos. Após ter visto um momento de esplendor na Grécia Antiga, tendo como nome principal **Aristóteles**, a Física entrou em declínio na Idade Média, tendo revivido apenas durante o **Renascimento** - o período da história da Europa, aproximadamente entre meados do século XIV e o fim do século XVI. Apesar das transformações serem bem evidentes na cultura, sociedade, economia, política e religião, caracterizando a transição do feudalismo para o capitalismo e significando uma evolução em relação às estruturas medievais, o termo é mais comumente empregado para descrever seus efeitos nas artes, na filosofia e nas ciências, no período marcado pela *Revolução Científica*.

## 1.1 Galileu Galilei

**Galileu Galilei** (1564-1642) é considerado o primeiro físico em seu sentido moderno, adotando a matemática como ferramenta principal.

A frase histórica de **Galileu** -

*"A verdade é filha do tempo, e não da autoridade. Se raciocinar fosse como carregar pedras, então vários raciocinadores seriam melhores que um. Mas raciocinar não é como carregar pedras. É como uma corrida, em que um único cavalo galopante supera facilmente uma centena de cavalos puxando carroças com pedras."*

**Galileu** foi um dos primeiros a descrever o real objetivo de um cientista: "*sua função é apenas descrever os fenômenos em vez de tentar explicá-los*". **Galileu Galilei** foi personalidade fundamental na *Revolução Científica*. Na história da ciência, chama-se *Revolução Científica* ao período que começou no século XVI e prolongou-se até o século XVIII. A partir desse período, a Ciência, que até então estava atrelada à Teologia, separa-se desta, e passa a ser um conhecimento mais estruturado e prático.





Figura 1 – Galileu Galilei - por Justus Sustermans 1636.

Fonte: <[https://pt.wikipedia.org/wiki/Galileu\\_Galilei](https://pt.wikipedia.org/wiki/Galileu_Galilei)>

Se o século XVIII foi o século da Mecânica clássica, do estudo das forças e do movimento de macro-objetos, o século XIX foi o estudo da Energia. Nos séculos XVIII e XIX surgiram os fundamentos da *termodinâmica* e do *eletromagnetismo*, destacando-se **Orsted** (1777-1851), **Ampère** (), **Charles** (), **Michael Faraday** (), **Nicolas Carnot** (1796-1832), **James Prescott Joule** (), **James Clerk Maxwell** (), **Rudolf Clausius** (), **Kelvin** (), e que realizou outra grande unificação da Física ao fundir eletricidade e magnetismo sob as mesmas descrições matemáticas, sendo que toda a Óptica pôde ser derivada da teoria eletromagnética de **Maxwell**.

Bem antes da adoção da teoria quântica, um dos principais problemas, do que agora é referido como a Física clássica, era a **natureza dupla da luz**. Enquanto sua propagação linear e a falta de um meio físico pareciam sugerir um comportamento semelhante a **partículas**, fenômenos como interferência e difração são propriedades bem conhecidas de **ondas**. E surgia a discussão se luz era partícula ou onda.

## 1.2 Huygens - 1690

Em 1690, **Christiaan Huygens** (1629-1695) explicou a *optical birefringence* em seu "*Trait'e de la lumière*", onde ele desenvolveu uma ampla teoria de ondas da luz (**HERMANN, 1978**). **Huygens** foi um físico, matemático e astrônomo holandês. Em Física, **Huygens** é bastante lembrado por seus estudos sobre luz e cores, percepção do som, estudo da força, entre outros.



Figura 2 – Christiaan Huygens - Em 1690, desenvolveu uma ampla teoria das ondas da luz.

Fonte: <[https://pt.wikipedia.org/wiki/Christiaan\\_Huygens](https://pt.wikipedia.org/wiki/Christiaan_Huygens)>

### 1.3 Newton - 1704

Já dotado de um método científico, a Física teve uma notável evolução com **Isaac Newton** (1643-1727), que realizou a primeira grande unificação da Física ao unir o *Espaço Cósmico* e a *Terra* sob as mesmas leis da Física, a *gravitação universal*.

Em 1704, 14 anos depois, **Isaac Newton** publicou seus "*Opticks*" em que explicou fenômenos como *reflexão*, *dispersão*, *cor* e *polarização* pela interpretação como um fluxo de partículas de tamanho diferente.

**Newton** desenvolveu, entre outras coisas, a teoria das cores baseada na observação que um prisma decompõe a luz branca em várias cores do espectro visível. Ele também formulou uma lei empírica de resfriamento e estudou a velocidade do som. Além de seu trabalho em *cálculo infinitesimal*, como matemático, **Newton** contribuiu para o estudo das *séries de potências*, generalizou o *teorema binomial* para expoentes não inteiros, e desenvolveu o *método de Newton* para a aproximação das raízes de uma função, além de muitas outras contribuições importantes.

### 1.4 Ampère

**André-Marie Ampère** (1775-1836) foi um físico, filósofo, cientista e matemático francês que fez importantes contribuições para o estudo do eletromagnetismo. Ocupou-se com vários ramos do conhecimento humano, deixando obras de importân-

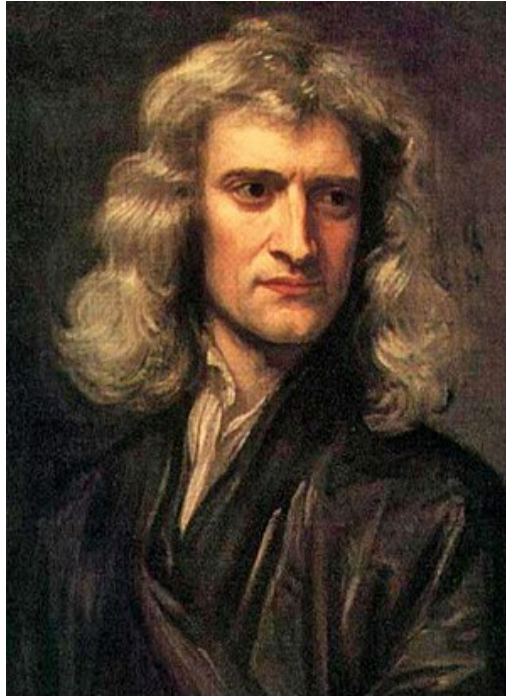


Figura 3 – Newton - Retratado por Godfrey Kneller, 1689, com 46 anos de idade.

Fonte: <[https://pt.wikipedia.org/wiki/Isaac\\_Newton](https://pt.wikipedia.org/wiki/Isaac_Newton)>



Figura 4 – Isaac Newton - Sua obra, *Princípios Matemáticos da Filosofia Natural* é considerada uma das mais influentes na história da ciência.

Fonte: <[https://pt.wikipedia.org/wiki/Isaac\\_Newton](https://pt.wikipedia.org/wiki/Isaac_Newton)>

cia, principalmente no domínio da Física e da Matemática. Partindo das experiências feitas pelo dinamarquês **Hans Christian Orsted** sobre o efeito magnético da corrente elétrica, soube estruturar e criar a teoria que possibilitou a construção de um grande número de aparelhos eletromagnéticos. Além disso, descobriu as leis que regem as atrações e repulsões das correntes elétricas entre si. Idealizou o galvanômetro, inventou o primeiro telégrafo elétrico e o eletroímã. Em sua homenagem, foi dado o nome de ampère (símbolo: A) à unidade de medida da intensidade de corrente elétrica.



Figura 5 – Ampère - Fez importantes contribuições para o estudo do eletromagnetismo.

Fonte: <[https://pt.wikipedia.org/wiki/Andre-Marie\\_Ampere](https://pt.wikipedia.org/wiki/Andre-Marie_Ampere)>

## 1.5 Thomas Young e Jean Fresnel

A *teoria corpuscular da luz* (a luz vista como partícula) dominou a discussão científica até o início do século XIX, quando **Thomas Young** e **Augustin Jean Fresnel** demonstraram várias deficiências da teoria que podem ser resolvidas assumindo ondas de luz, transversal, em um meio universal chamado *Ether*.

**Thomas Young** (1773-1829) foi um físico britânico. Em 1801 foi nomeado professor de filosofia natural do Royal Institution. Conhecido pela *experiência da dupla fenda*, que possibilitou a determinação do carácter ondulatório da luz.



Figura 6 – Thomas Young - Juntamente com Fresnel demonstrou várias deficiências da teoria corpuscular da luz.

Fonte: <[https://pt.wikipedia.org/wiki/Thomas\\_Young](https://pt.wikipedia.org/wiki/Thomas_Young)>

**Augustin-Jean Fresnel** (1788-1827) foi um físico francês. **Fresnel** contribuiu significativamente para a *teoria da óptica ondulatória*. Estudou o comportamento

da luz, tanto teórico, como experimentalmente. É considerado o fundador da óptica moderna.



Figura 7 – Augustin Fresnel - Trabalhando com Young, demonstrou várias deficiências da teoria corpuscular da luz, que podem ser resolvidas assumindo ondas de luz, transversal, em um meio universal chamado Ether.

Fonte: <[https://pt.wikipedia.org/wiki/Augustin\\_Jean\\_Fresnel](https://pt.wikipedia.org/wiki/Augustin_Jean_Fresnel)>

## 1.6 Charles - 1787

**Jacques Alexandre César Charles** (1746-1823) foi um importante químico e físico que estudou os gases. Desenvolveu a teoria que leva o seu nome, a Lei de Charles. Por volta de 1787, Charles desenvolveu sua teoria, a *Lei de Charles*. Ele não chegou a publicá-la mas **Gay-Lussac** a publicou quinze anos depois. Seus trabalhos eram baseados no estudo dos gases. Ele redesenhou a forma como balões de ar quente foram construídos. Inventou a linha de válvulas dentre outros equipamentos para acondicionamento de gases. Mas a sua invenção mais conhecida, sem dúvida foi a **Lei de Charles**, que diz que a um volume constante, a pressão de uma determinada massa de gás é diretamente proporcional à sua temperatura absoluta, ou seja, constante. Esta é uma das leis dos gases perfeitos ou gás ideal.

## 1.7 Orsted - 1806

**Hans Christian Orsted** (1777-1851) foi um físico e químico dinamarquês. É conhecido sobretudo por ter descoberto que as correntes elétricas podem criar campos magnéticos que são parte importante do Eletromagnetismo. Na Alemanha começou a acreditar na existência de uma ligação entre eletricidade e magnetismo. A existência dessa ligação fez sentido para **Orsted**, uma vez que acreditava na unidade da natureza, e, como tal, que haveria necessariamente uma ligação entre muitos fenômenos naturais. Essas pressuposições levaram **Orsted** ao estudo da Física. Tornou-se professor na Universidade de Copenhague em 1806 e continuou a sua pesquisa sobre a *corrente elétrica* e a *acústica*.



Figura 8 – Charles - A um volume constante, a pressão de uma determinada massa de gás é diretamente proporcional à sua temperatura absoluta.

Fonte: <[en.wikipedia.org](http://en.wikipedia.org)>, <[http://soq.com.br/biografias/jacques\\_charles/](http://soq.com.br/biografias/jacques_charles/)>

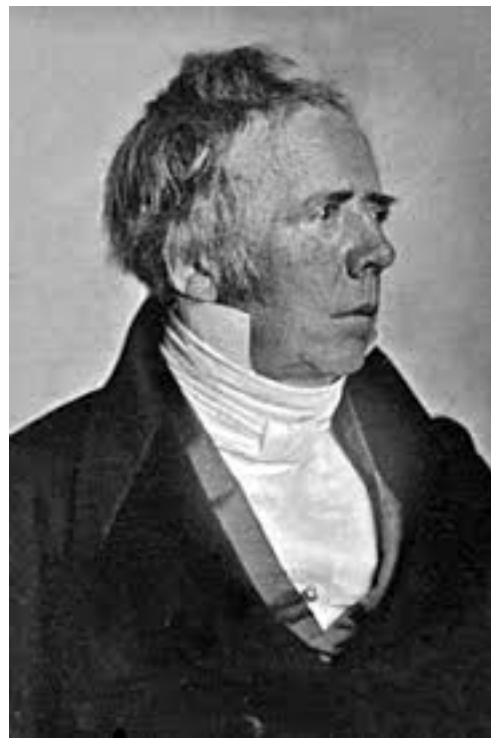


Figura 9 – Orsted - A ligação entre eletricidade e magnetismo.

Fonte: <[https://pt.wikipedia.org/wiki/Hans\\_Christian\\_Orsted](https://pt.wikipedia.org/wiki/Hans_Christian_Orsted)> <[en.wikipedia.org](http://en.wikipedia.org)>

## 1.8 Carnot - 1824

A Termodinâmica se inicia como ciência. Em 1824, **Nicolas Carnot** (1796-1892), um físico, matemático e engenheiro francês, estudou os primeiros problemas em um modo científico e matemático.

A **Primeira Lei da Termodinâmica** determina, basicamente, que "**a energia se conserva**". Isso quer dizer que **nos processos físicos a energia não se perde, ela se converte de um tipo em outro**. Por exemplo, uma máquina utiliza energia para realizar trabalho e nesse processo a máquina aquece. Ou seja, a energia mecânica está sendo degradada em energia térmica. A energia térmica não se transforma novamente em energia mecânica (se isso acontecesse a máquina nunca deixaria de funcionar), portanto *o processo é irreversível*.



Figura 10 – Carnot e Primeira Lei da Termodinâmica - Nos processos físicos a energia não se perde, ela se converte em um outro tipo de energia.

Fonte: [https://pt.wikipedia.org/wiki/Nicolas\\_Léonard\\_Sadi\\_Carnot](https://pt.wikipedia.org/wiki/Nicolas_Léonard_Sadi_Carnot)

**Carnot** foi quem deu o primeiro modelo teórico de sucesso sobre as máquinas térmicas, o *ciclo de Carnot*, e apresentou os fundamentos da **Segunda Lei da Termodinâmica**. Em suas pesquisas sobre transformação da energia mecânica em térmica, e vice-versa, ele constatou que seria impossível que existisse uma máquina com eficiência total.

Até meados do século XIX, acreditava-se ser possível a construção de uma máquina térmica ideal, que seria capaz de transformar toda a *energia* fornecida em *trabalho*, obtendo um rendimento total (100%). Para demonstrar que não seria possível, **Nicolas Carnot** propôs uma máquina térmica teórica que se comportava como uma máquina de rendimento total, estabelecendo um ciclo de rendimento máximo, que mais tarde passou a ser chamado *Ciclo de Carnot*. **Carnot** concluiu que para que houvesse 100% de rendimento, todo o calor vindo de uma fonte de aquecimento deveria ser transformado em trabalho, pois a temperatura absoluta de uma fonte de resfriamento deveria ser 0K (zero graus Kelvin). Partindo daí concluiu que o zero absoluto não é possível para um sistema físico. O conceito de *entropia* começava a ser desenvolvido por **Carnot**.

## 1.9 Faraday - 1831

**Michael Faraday** (1791-1867) foi um físico e químico inglês. As descobertas de Faraday cobrem áreas significativas das modernas física e química, e a tecnologia desenvolvida baseada no seu trabalho está ainda mais presente (ALVES, 2017). Suas descobertas em eletromagnetismo forneceram a base para os trabalhos de engenharia no fim do século XIX para que **Edison**, **Siemens**, **Tesla** e **Westinghouse** tornassem possível a eletrificação das sociedades industrializadas.

Na física, foi um dos primeiros a estudar as relações entre eletricidade e magnetismo. Em 1821, logo após **Oersted** descobrir que a eletricidade e o magnetismo eram associados entre si, **Faraday** publicou um trabalho que chamou de *rotação eletromagnética*, elaborando os princípios de funcionamento do motor elétrico. Em 1831, **Faraday** descobriu a indução eletromagnética, o princípio por trás do gerador elétrico e do transformador elétrico. Suas ideias sobre os campos elétricos e os magnéticos, e a natureza dos campos em geral, inspiraram trabalhos posteriores fundamentais nessa área, como as equações de **Maxwell**. Seus estudos sobre campos eletromagnéticos são conceitos-chave da física atual.

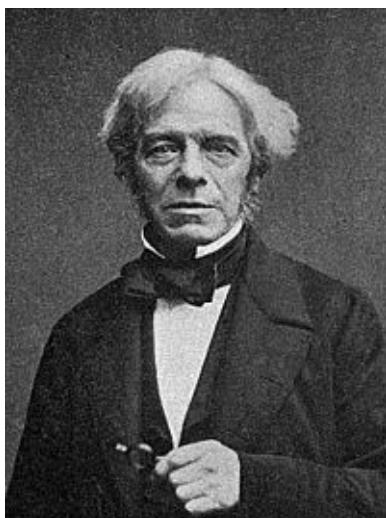


Figura 11 – Faraday - Um pioneiro no estudo da eletricidade e magnetismo e descobridor da indução eletromagnética.

Fonte: <[https://pt.wikipedia.org/wiki/Michael\\_Faraday](https://pt.wikipedia.org/wiki/Michael_Faraday)>

Seus trabalhos em eletroquímica são amplamente usados em química industrial. Talvez a sua maior contribuição tenha sido virtualmente fundar a *eletroquímica*. **Faraday** criou termos como eletrólito, ânodo, catodo, eletrodo, e íon (ALVES, 2017).

## 1.10 Balmer - 1848

**Johann Balmer** (1825-1898) (na Figura 12) foi um físico e matemático suíço. Seu nome é particularmente conhecido pela descoberta da fórmula que determina o comprimento das linhas espectrais do hidrogênio atômico em 1848. Na época, **Balmer** conseguiu encontrar uma equação matemática muito simples para descrever



o comprimento de onda associado às raias produzidas pela emissão de uma lâmpada de hidrogênio ao atravessar um prisma.



Figura 12 – Johann Balmer - O primeiro indício da "revolução quântica" surgiu em 1885 com Balmer.

Fonte: <[https://pt.wikipedia.org/wiki/Johann\\_Jakob\\_Balmer](https://pt.wikipedia.org/wiki/Johann_Jakob_Balmer)>

O primeiro indício da "revolução quântica" surgiu em 1885 com **Balmer** (COBO; ZANATTA, 2013).

### 1.11 Joule - 1849

**James Prescott Joule** (1818-1889) foi um físico britânico. Em 1849, Joule demonstrou a equivalência entre trabalho e calor, ao medir o aumento da temperatura de uma amostra de água quando uma roda de pás é rotacionada dentro dessa amostra <<https://pt.wikipedia.org/wiki/Joule>>. Referente ao seu nome o termo "joules" é a unidade tradicionalmente usada para medir energia mecânica (trabalho), também utilizada para medir energia térmica (calor). No Sistema Internacional de Unidades (SI), todo trabalho ou energia são medidos em joules.

### 1.12 Clausius - 1850 e 1865

**Rudolf Julius Emanuel Clausius** (1822-1888) foi um físico e matemático alemão, considerado um dos fundadores centrais da ciência da termodinâmica. Por reafirmar o princípio de **Carnot** conhecido como *ciclo de Carnot*, ele pôs a teoria do calor numa base mais sólida e mais verdadeira. Em seu artigo mais importante, Sobre a teoria mecânica do calor, publicado em 1850, expôs pela primeira vez as ideias básicas da Segunda lei da termodinâmica. **Clausius** demonstrou que

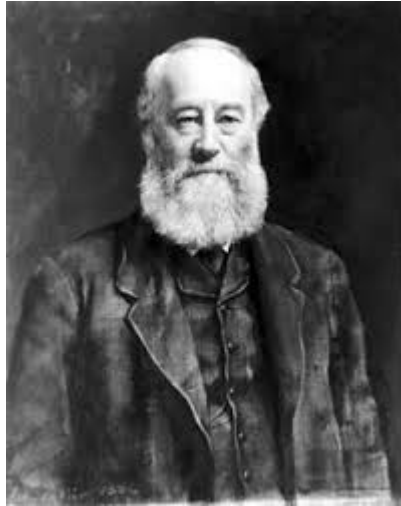


Figura 13 – James Joule - A equivalência entre trabalho e calor.

Fonte: <<https://pt.wikipedia.org/wiki/Joule>> ,

era possível compatibilizar o Princípio de Carnot com a Teoria Cinética dos Gases, se a conservação do calor se transformasse no princípio de conservação de energia.

Em 1865, **Clausius** introduziu o conceito de entropia. A *entropia* seria a **medida da quantidade de energia térmica que não pode ser revertida em energia mecânica** (não pode realizar trabalho) em uma determinada temperatura. **Clausius** desenvolveu uma fórmula matemática para a variação da entropia ( $\Delta S$ ) que é utilizada atualmente, em função de  $Q$ , o calor transferido e,  $T$  a temperatura.



Figura 14 – Rudolf Clausius - Introduziu o conceito de entropia, a medida da quantidade de energia térmica que não pode ser revertida em energia mecânica.

Fonte: <[https://pt.wikipedia.org/wiki/Rudolf\\_Clausius](https://pt.wikipedia.org/wiki/Rudolf_Clausius)> ,

A *entropia* é uma grandeza termodinâmica que mensura o *grau de irreversibilidade de um sistema*, encontrando-se geralmente associada ao que se denomina por "desordem" de um sistema termodinâmico. *Entropia* é a medida do grau de desordem de

um sistema. É uma grandeza física que está relacionada com a **Segunda Lei da Termodinâmica** e que tende a aumentar naturalmente num sistema termodinâmico. A "desordem" não deve ser compreendida como "bagunça" e sim como a forma de organização das moléculas no sistema. Um exemplo simples para entender a desordem das moléculas em um sistema é o gelo que derrete. As moléculas no estado sólido estão mais próximas e têm menor possibilidade de movimentação, portanto elas estão mais organizadas.

### 1.13 Kelvin

**Lord Kelvin** (1824-1907) foi um matemático e físico irlandês, cujo nome verdadeiro era **William Thomson**. Veja **Kelvin** na Figura 15. Aos 68 anos de idade, receberia o título de nobreza de Primeiro Barão Kelvin de Largs, pela grande importância de seu trabalho científico. As propriedades do calor foram um dos sistemas preferidos de **Kelvin**. Analisou com mais profundidades as descobertas de **Jacques Charles** sobre a variação de volume dos gases em função da variação da temperatura. **Charles** concluiu, com base em experimentos e cálculos, que **à temperatura de  $-273^{\circ}C$  todos os gases teriam volume igual a zero**. **Kelvin** propôs outra conclusão: **não era o volume da matéria que se anularia nessa temperatura, mas sim a energia cinética de suas moléculas**. Sugeriu então que essa temperatura deveria ser considerada a mais baixa possível e chamou-a de *zero absoluto*. A partir dela, propôs uma nova escala termométrica (que posteriormente recebeu o nome de escala Kelvin), a qual permitiria maior simplicidade para a expressão matemática das relações entre grandezas termodinâmicas. **Kelvin** também concluiu, analisando os trabalhos do francês **Carnot**, que **era impossível utilizar toda a energia de um sistema na forma de trabalho**. Uma parte dessa energia é inevitavelmente perdida na forma de calor. Mais tarde o **Lord Kelvin** complementou as pesquisas de **Carnot** sobre a *irreversibilidade dos processos termodinâmicos*, dando origem às bases da **Segunda Lei da Termodinâmica**.



Figura 15 – Lord Kelvin - Complementou as pesquisas de Carnot sobre a irreversibilidade dos processos termodinâmicos, dando origem às bases da Segunda Lei da Termodinâmica.

Fonte: <[https://pt.wikipedia.org/wiki/William\\_Thomson](https://pt.wikipedia.org/wiki/William_Thomson)> ,

## 1.14 Gustav Kirchhoff - 1859

**Gustav Robert Kirchhoff** (1824-1887) foi um físico nascido na antiga Prússia em Königsberg, atualmente Kaliningrado, Rússia. Suas contribuições científicas foram principalmente no campo dos circuitos elétricos, na espectroscopia, na emissão de radiação dos corpos negros e na teoria da elasticidade (modelo de placas de **Kirchhoff-Love**). **Kirchhoff** propôs o nome de **radiação do corpo negro** em 1862. É autor de duas leis fundamentais da teoria clássica dos circuitos elétricos e da emissão térmica. **Kirchhoff** formulou as leis dos nodos e das malhas na análise de circuitos elétricos (Leis de Kirchhoff) em 1845, quando ainda era um estudante. Propôs a lei da *emissão de radiação térmica* em 1859, comprovando-a em 1861. Em 1854 transferiu-se para a Universidade de Heidelberg, onde colaborou em trabalhos sobre espectroscopia com **Robert Bunsen** (um químico alemão), descobrindo juntamente com este, os elementos céσιο e rubídio em 1861.

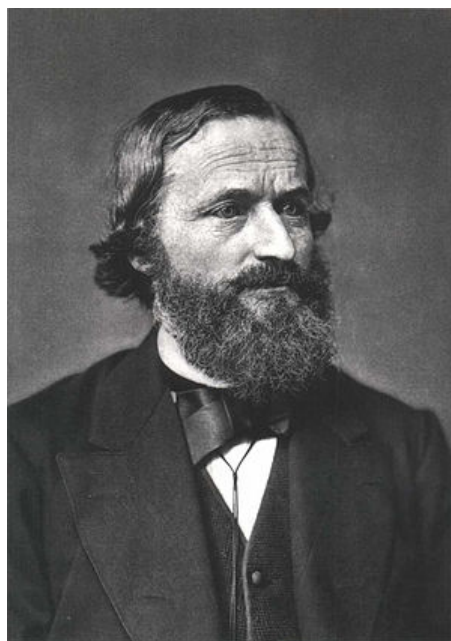


Figura 16 – Kirchhoff - O pioneiro no estudo da emissão de radiação de um corpo negro.

Fonte: <[https://pt.wikipedia.org/wiki/Gustav\\_Kirchhoff](https://pt.wikipedia.org/wiki/Gustav_Kirchhoff)>

Posteriormente propôs as três leis que descrevem a *emissão de luz por objetos incandescentes*:

1. Um objeto sólido aquecido produz luz com espectro contínuo.
2. Um gás ténue produz luz com linhas espectrais em comprimentos de onda discretos que dependem da composição química do gás.
3. Um objeto sólido a alta temperatura rodeado de um gás ténue a temperaturas inferiores produz luz num espectro contínuo com vazios em comprimentos de onda discretos cujas posições dependem da composição química do gás.

A existência destas leis foi explicada mais tarde por **Niels Bohr**, contribuindo decisivamente para o nascimento da **mecânica quântica**. Seu livro "Vorlesungen über mathematische Physik, Mechanik", 1897, é actualmente fonte básica de referência.

A Lei de **Kirchhoff** para radiação térmica é uma declaração geral igualando emissão e absorção em objetos aquecidos, proposta por Kirchhoff em 1859 (e demonstrada em 1861), a partir de considerações gerais de equilíbrio termodinâmico.

Um objeto a uma temperatura diferente de zero irradia **energia eletromagnética**. Se esse objeto é um **corpo negro** perfeito, absorvendo toda a luz que incide sobre ele, ele irradia energia de acordo com a fórmula de radiação do corpo negro. De maneira geral, ele irradia com alguma emissividade multiplicada pela fórmula do corpo negro. A lei de Kirchhoff declara: "em equilíbrio térmico, a emissividade de um corpo (ou superfície) é igual a seu poder de absorção.

## 1.15 Maxwell - 1864 e 1873

**James Clerk Maxwell** (1831-1879) foi um físico e matemático escocês. É mais conhecido por ter dado forma final à teoria moderna do eletromagnetismo, que une a eletricidade, o magnetismo e a óptica. Esta é a teoria que surge das equações de Maxwell, assim chamadas em sua honra e porque foi o primeiro a escrevê-las juntando a lei de **Ampère** modificada por **Maxwell**, a lei de **Gauss**, e a lei da indução de **Faraday**. **Maxwell** demonstrou que os campos elétricos e magnéticos se propagam com a velocidade da luz. Ele apresentou uma teoria detalhada da luz como um efeito electromagnético, isto é, que a luz corresponde à propagação de ondas eléctricas e magnéticas, hipótese que tinha sido posta por Faraday. Foi demonstrado em 1864 que as forças eléctricas e magnéticas têm a mesma natureza: uma força eléctrica em determinado referencial pode tornar-se magnética se analisada noutra, e vice-versa. Ele também desenvolveu um trabalho importante em mecânica estatística, estudou a teoria cinética dos gases e descobriu a distribuição de **Maxwell-Boltzmann**. Seu trabalho em eletromagnetismo foi a base da relatividade restrita de **Einstein** e o seu trabalho em teoria cinética de gases fundamental ao desenvolvimento posterior da mecânica quântica.

Em 1873 em seu *Tratado sobre Eletricidade e Magnetismo*, **Maxwell** publicou um conjunto de 4 equações diferenciais parciais que lançam as bases para a eletrodinâmica clássica e, elegantemente, explica a luz como ondas eletromagnéticas. A teoria de **Maxwell**, contudo, ainda era incapaz de explicar a radiação dos corpos negros, bem como o espectro de energia discreta de átomos.

## 1.16 John Strutt (Lord Rayleigh) - 1877 e 1889

**John William Strutt** (1842-1919), um matemático e físico inglês, de cognome terceiro **Baron Rayleigh**, foi um dos poucos membros da alta nobreza britânica que ganhou fama como um cientista excepcional. **Strutt** era conhecido por suas pesquisas em fenômenos ondulatórios. As primeiras pesquisas de **Lord Rayleigh** foram principalmente matemáticas, relativas a ótica e sistemas vibratórios, mas seu trabalho posterior abrange quase todo o campo da Física, abrangendo som, teoria de onda, visão de cores, eletrodinâmica, eletromagnetismo, dispersão de luz, fluxo de líquidos, hidrodinâmica, densidade, de gases, viscosidade, capilaridade,



Figura 17 – Maxwell - É mais conhecido por ter dado forma final à teoria moderna do eletromagnetismo, que une a eletricidade, o magnetismo e a óptica.

Fonte: <[https://pt.wikipedia.org/wiki/James\\_Clerk\\_Maxwell](https://pt.wikipedia.org/wiki/James_Clerk_Maxwell)>

elasticidade e fotografia. Seus experimentos levaram ao estabelecimento dos padrões de resistência, corrente e força eletromotriz; e seu trabalho posterior foi concentrado em problemas elétricos e magnéticos. **Lord Rayleigh** foi um excelente instrutor e, sob sua supervisão ativa, um sistema de instrução prática em Física experimental foi criado em Cambridge, desenvolvendo-se de uma classe de cinco ou seis alunos a uma escola avançada de cerca de setenta físicos experimentais. Sua *teoria do som* foi publicada em dois volumes durante 1877-1878.

Mas, o problema desafiador, tratava da radiação provenientes de objetos incandescentes. Neste caso a questão parecia ser relativamente simples, uma vez que o resultado deveria ser função exclusiva da temperatura do objeto. Contudo, os trabalhos realizados por **Strutt** (*Lord Rayleigh*) deixaram evidentes várias inconsistências entre os resultados experimentais e os modelos (clássicos) utilizados. Na época, era evidente que o fenômeno devia-se às características dos átomos considerados, mas as características e o processo associado, no entanto, não eram conhecidos.

Outros estudos extensivos de **Strutt** são relatados em seus trabalhos científicos - seis volumes publicados durante 1889-1920. Ele também contribuiu para a Enciclopédia Britânica. **John William Strutt** foi Prêmio Nobel de Física em 1904.

## 1.17 Os resultados de Stefan-Boltzmann - 1879

Em 1879, o físico esloveno **Jozef Stefan** (1835-1893) deduziu, a partir de resultados experimentais, que a potência  $P$  (energia irradiada por segundo) de um corpo negro é diretamente proporcional à sua temperatura  $T$  elevada à quarta



Figura 18 – John Strutt - as evidências de inconsistências entre trabalhos experimentais e o modelos matemáticos clássicos utilizados.

Fonte: <[https://pt.wikipedia.org/wiki/John\\_William\\_Strutt](https://pt.wikipedia.org/wiki/John_William_Strutt)>

potência e também diretamente proporcional à área  $A$  da superfície emissora. Essa relação foi chamada de *Lei de Stefan*.



Figura 19 – Jozef Stefan - Em 1879 estabeleceu que a radiação total de um corpo negro é proporcional à quarta potência de sua temperatura.

Fonte: <[https://pt.wikipedia.org/wiki/Joseph\\_Stefan](https://pt.wikipedia.org/wiki/Joseph_Stefan)>

$$P = \sigma \cdot T^4$$

Onde  $\sigma = 5,67 \times 10^{-8} \text{ W/m}^2 \text{ K}^4$  é a *constante de Stefan*.

Apoiando-se nas leis da termodinâmica e da eletrodinâmica de **Maxwell**, o físico austríaco **Ludwig Boltzmann** (1844-1906) desenvolveu em 1884, a fundamentação teórica da *Lei de Stefan*. A Lei de **Stefan-Boltzmann** pode ser assim enunciada: a *potência* total da radiação emitida (a área sob a curva) aumenta com a temperatura.

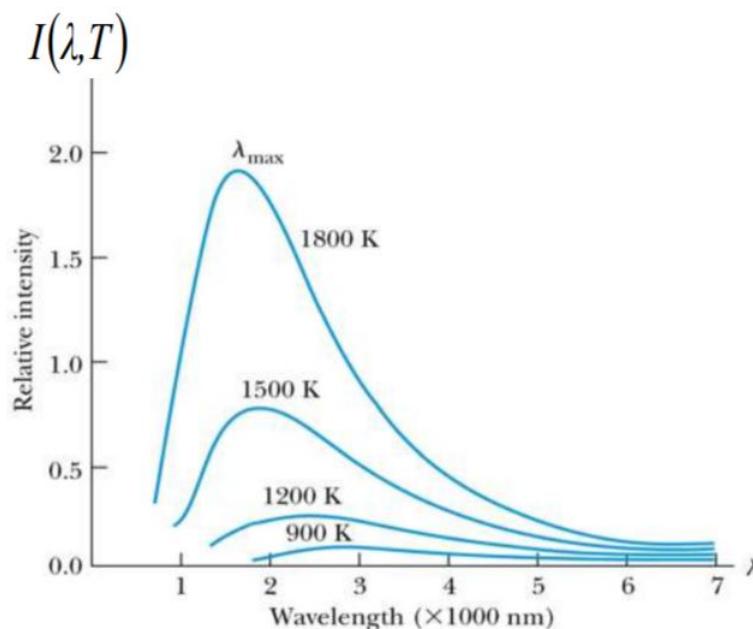


Figura 20 – Lei de Stefan-Boltzmann - A *potência* total da radiação emitida (a área sob a curva) aumenta com a temperatura.

Fonte: <[http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo\\_negro.pdf](http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo_negro.pdf)>

## 1.18 Rydberg e os comprimentos de onda de fótons - 1888

**Johannes Robert Rydberg** (1854-1919) foi um físico sueco. É conhecido principalmente pela concepção da fórmula de **Rydberg**, em 1888, usada para fazer previsão dos comprimentos de onda da radiação de fótons (de luz e outras radiações eletromagnéticas) emitidos devido a alterações do nível de energia de um elétron num átomo.

A fórmula de *Rydberg* (fórmula de Rydberg-Ritz) ou equação de **Rydberg** é utilizada em física atômica para determinar todo o espectro da luz emitida pelo hidrogênio, posteriormente estendida para uso com qualquer elemento químico. O espectro é o conjunto de comprimentos de onda dos fótons emitidos quando o elétron pula entre níveis de energia discretos, "camadas" ao redor do átomo de um certo elemento químico. **A descoberta posteriormente promoveu motivação para a criação da Física Quântica.** A fórmula foi inventada pelo físico sueco **Johannes Rydberg** e apresentada em 5 de novembro de 1888. Ver o trabalho de **Rydberg** em ([GALLAS, 1986](#)).

O resultado de **Balmer** foi complementado e adaptado em 1888 pelo físico sueco **Johannes Rydberg** (1854-1919) que, já há algum tempo, vinha trabalhando sobre





Figura 21 – Ludwig Boltzmann aos 24 anos em 1869 - Leis da radiação de um corpo negro, juntamente com Jozef Stefan.

Fonte: <[https://pt.wikipedia.org/wiki/Ludwig\\_Boltzmann](https://pt.wikipedia.org/wiki/Ludwig_Boltzmann)>



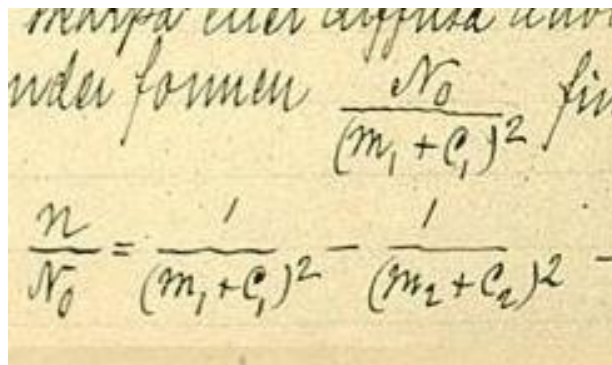
Figura 22 – Rydberg - A previsão dos comprimentos de onda da radiação de fótons.

Fonte: <[https://pt.wikipedia.org/wiki/Johannes\\_Rydberg](https://pt.wikipedia.org/wiki/Johannes_Rydberg)>

os espectros de emissão de metais alcalinos (RYDBERG, 1888). É conhecido principalmente pela concepção da fórmula de **Rydberg** em 1888, usada para fazer previsão dos comprimentos de onda de fótons (de luz e outras radiações electromagnéticas) emitidos devido a alterações do nível de energia de um elétron num átomo.

### 1.19 Wilhelm Wien - 1893

Um outro resultado também relevante é a **Lei dos Deslocamentos de Wien**. **Wilhelm Wien** (1864-1928) um físico alemão que, em 1893, usou as teorias



Handwritten formula for the Rydberg constant, showing the relationship between the Rydberg constant  $R_0$  and the masses and charges of two particles:

$$\frac{R}{R_0} = \frac{1}{(m_1 + e_1)^2} - \frac{1}{(m_2 + e_2)^2}$$

Figura 23 – Fórmula de Rydberg - Um pedaço do documento original que detalha a fórmula de Rydberg.

Fonte: <[https://pt.wikipedia.org/wiki/Johannes\\_Rydberg](https://pt.wikipedia.org/wiki/Johannes_Rydberg)>



Figura 24 – Rydberg - O trabalho sobre espectros de emissão de metais alcalinos.

Fonte: <[https://pt.wikipedia.org/wiki/Johannes\\_Rydberg](https://pt.wikipedia.org/wiki/Johannes_Rydberg)>

sobre o calor e eletromagnetismo para deduzir a lei do deslocamento de **Wien**, que calcula a emissão de um corpo negro a qualquer temperatura a partir da emissão em qualquer uma temperatura de referência. Ele descobriu que a *intensidade máxima* da radiação de corpo negro desloca-se para comprimentos de onda menores (a frequências maiores) à medida que o corpo é aquecido. Veja o  $\lambda_{max}$  na Figura . Os resultados foram fundamentais para a formulação da Mecânica Quântica. **Wien** em 1911 recebeu o Prêmio Nobel por seu trabalho sobre a radiação do calor.

## 1.20 JJ Thomson -1897

**Joseph John Thomson**, mais conhecido como J. J. Thomson, foi um físico britânico que descobriu o elétron. Estudou engenharia no Owens College e depois no Trinity College em Cambridge. Em 1897, **JJ Thomson** (1856-1940) descobriu o *elétron*, a primeira partícula subatômica descoberta. Pela descoberta dos elétrons, **J.J. Thomson** recebeu o Nobel de Física de 1906.

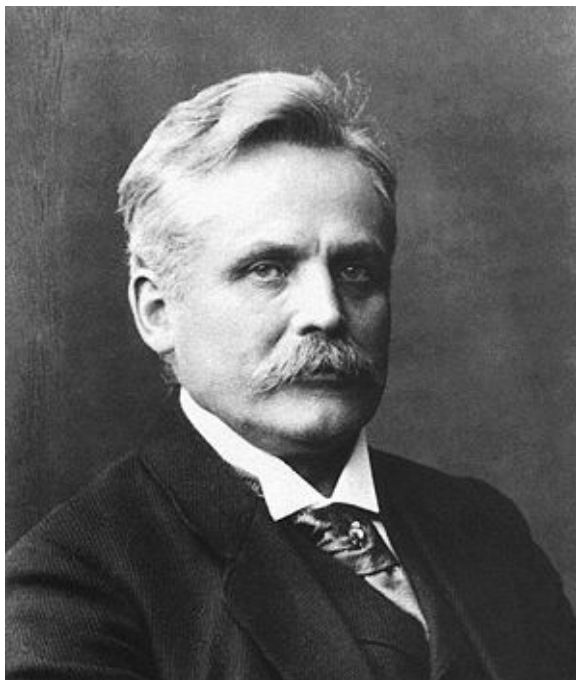


Figura 25 – Wilhelm Wien - A intensidade máxima da radiação de um corpo negro desloca-se para comprimentos de onda menores e frequências maiores.

Fonte: <[https://pt.wikipedia.org/wiki/Wilhelm\\_Wien](https://pt.wikipedia.org/wiki/Wilhelm_Wien)>



Figura 26 – J. J. Thomson - O descobridor do elétron em 1897.

Fonte: <<https://www.misteriosdouniverso.net/2016/10/20-fisicos-que-revolucionaram-nossa.html>>

As experiências de **Thomson** podem ser consideradas o início do entendimento da estrutura atômica. Suas experiências com o tubo de raios catódicos permitiu concluir irrefutavelmente a existência dos elétrons. Com a descoberta dos elétrons de carga negativa, concluiu-se também a existência dos prótons. Isso originava um modelo

de átomo constituído de carga elétrica positiva (prótons), que continha elétrons de carga negativa.

## 1.21 Lummer e Pringshein, 1899, as primeiras medidas de um corpo negro

Era 1899. Na época, muitos pesquisadores dedicaram-se a medir e descrever a *distribuição de energia emitida por corpos negros* em diferentes temperaturas. As primeiras medidas precisas foram dos físicos alemães **Otto Richard Lummer** (1860-1925) e **Ernst Pringshein** (1859-1917) que ocorreram em 1899. Embora as principais propriedades fossem conhecidas, a Física clássica não oferecia meios de descrever a distribuição por inteiro <[http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo\\_negro.pdf](http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo_negro.pdf)>.



Figura 27 – Lummer em 1902 - Primeiras medidas de energia emitida por um corpo negro.

Fonte: <[https://pt.wikipedia.org/wiki/Otto\\_Lummer](https://pt.wikipedia.org/wiki/Otto_Lummer)>

## 1.22 O início da mecânica quântica

No fim do século XIX, a história da mecânica quântica, entrelaçada com a história da química quântica, começa essencialmente com o descobrimento dos raios catódicos em 1838 realizado por **Michael Faraday**, a introdução do termo *corpo negro* por **Gustav Kirchhoff** no inverno de 1859-1860, e a sugestão feita por **Ludwig Boltzmann** em 1877 sobre que os estados de energia de um sistema físico deveriam ser discretos. A história começa em 1879 com Stefan-Boltzmann, seguido por **Rydberg** (1854-1919) em 1888, o trabalho de **Wilhelm Wien** em 1893 e, depois por **Lummer e Pringshein** em 1899. Em 1900, surge a *Lei de Rayleigh-Jeans*.

Quando o século XIX chegava ao fim, os físicos ao redor do mundo começavam a pensar que sua época já havia passado. A Física teria acabado e os físicos deveriam

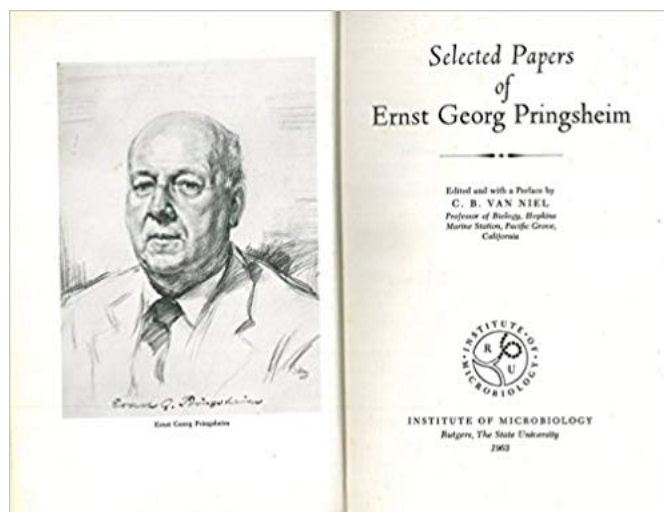


Figura 28 – Pringsheim - Juntamente com Lummer, as primeiras medidas de energia emitida por um corpo negro.

Fonte: Google Images <[amazon.com](https://www.amazon.com)>

buscar novas carreiras. Naquela época, o sentimento é que o futuro da Física consistiria, somente, na tarefa de medir as constantes físicas do universo, com níveis cada vez maiores de exatidão. Mesmo assim, havia, aparentemente, problemas menores que ainda esperavam uma solução. Uma das questões em aberto se relacionava com o modo como um objeto emitia radiação.

No final do século XIX pensava-se que todos os fenômenos físicos poderiam ser explicados dentro das teorias correntes. Entretanto, certos "fenômenos rebeldes" fugiam do alcance dos cientistas. Fatos que a Física clássica não podia explicar:

- O espectro do corpo negro;
- Os espectros de linhas atômicas;
- A estabilidade do átomo.

No âmbito científico um *espectro* é uma representação das amplitudes ou intensidades - o que geralmente traduz-se por energia - dos componentes ondulatórios de um sistema quando discriminadas uma das outras em função de suas respectivas frequências (ou comprimentos de onda). Em um espectro as componentes ondulatórias (fases) distinguem-se fisicamente umas das outras não por suas naturezas, mas sim, pelas suas frequências.

A *radiação eletromagnética* é uma oscilação em fase dos *campos elétricos e magnéticos* que, autossustentando-se, encontram-se desacoplados das cargas elétricas que lhe deram origem. As oscilações dos campos magnéticos e elétricos são perpendiculares entre si e podem ser entendidas como a propagação de uma onda transversal, cujas oscilações são perpendiculares à direção do movimento da onda (como as ondas da superfície de uma lâmina de água), que pode se deslocar através do vácuo. Dentro do ponto de vista da mecânica quântica, podem ser entendidas, ainda, como *o deslocamento de pequenas partículas, os fótons*. O espectro visível, ou simplesmente luz

visível, é apenas uma pequena parte de todo o espectro da radiação eletromagnética possível, que vai desde as ondas de rádio aos raios gama. A existência de ondas eletromagnéticas foi prevista por **James Clerk Maxwell** e confirmada experimentalmente por **Heinrich Hertz**. A radiação eletromagnética encontra aplicações como a radiotransmissão, seu emprego no aquecimento de alimentos (fornos de micro-ondas), em lasers para corte de materiais ou mesmo na simples lâmpada incandescente.

A *radiação térmica* é a radiação eletromagnética gerada pelo movimento térmico das partículas carregadas na matéria. Toda matéria com uma temperatura maior que o zero absoluto emite radiação térmica. O movimento de partículas resulta em aceleração que produz radiação eletromagnética; no entanto, uma interferência destrutiva pode cancelar toda a radiação. Muitas vezes a **radiação térmica é chamada de radiação de corpo negro**, uma radiação eletromagnética-térmica dentro ou ao redor de um corpo, em que um objeto emissor de radiação atende às características físicas de um corpo negro em equilíbrio termodinâmico. Exemplos de radiação térmica incluem a luz visível e a luz infravermelha emitidas por uma lâmpada incandescente. Sobre um *corpo negro*, o que realmente ocorre quando um objeto é aquecido a temperaturas cada vez mais altas é que, em princípio, a maior parte da energia é irradiada como infravermelho. Após um determinado aquecimento o corpo começa a brilhar em vermelho visível incandescente e se o aquecimento continuar, teremos laranja, e azul esbranquiçado. Quanto mais quente o corpo, menor é o comprimento de onda que a maior parte de sua energia é irradiada. Ainda que um pouco da energia seja irradiada em comprimentos de onda maiores e menores, o pico de emissão de um *corpo negro* é centrado em uma faixa estreita de comprimento de onda, que depende apenas da temperatura.

- A radiação emitida por um corpo devido à sua temperatura é chamada radiação térmica;
- Se um corpo tiver temperatura maior que a ambiente, ele irradia, caso contrário ele absorve;
- Um *corpo negro* é qualquer corpo que absorve toda a radiação incidente sobre ele.

## 1.23 Rayleigh-Jeans e a distribuição espectral de um corpo negro

**James Hopwood Jeans** (1877-1946) foi um físico, astrônomo e matemático britânico, que juntamente com **Rayleigh**, ajudou a descobrir a lei de *Rayleigh-Jeans* (1900).

Fórmula **Rayleigh-Jeans** (1900-1905) - **Lord Rayleigh** usou as teorias clássicas do eletromagnetismo e da termodinâmica para mostrar que a *distribuição espectral de um corpo negro* deveria ser:

Onde  $I$  é função de  $\lambda$  e  $T$ . Para *comprimentos de ondas grandes* esta equação se ajusta aos resultados experimentais, mas para os *comprimentos de onda curtos* há uma discordância muito grande entre esta teoria e a experiência. Esta discordância é chamada de **catástrofe do ultravioleta**. A lei agregava umas medidas experimentais para comprimentos de onda. Entretanto, esta predizia uma produção de energia

$$I = \frac{2\pi c k T}{\lambda^4}$$

Figura 29 – Fórmula de Rayleigh-Jeans para mostrar a distribuição espectral de um corpo negro.

Fonte: <[http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo\\_negro.pdf](http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo_negro.pdf)>



Figura 30 – John William Strutt - Prêmio Nobel de Física em 1904.

Fonte: <[https://www.nobelprize.org/nobel\\_prizes/physics/laureates/1904/strutt-bio.html](https://www.nobelprize.org/nobel_prizes/physics/laureates/1904/strutt-bio.html)>

que tendia ao infinito já que o comprimento de onda se fazia cada vez menor. Esta ideia não se sustentava pelos experimentos e a falha se conheceu como a "catástrofe ultravioleta"; entretanto, não foi, como as vezes se afirma nos livros-texto de Física, uma motivação para a *teoria quântica*. Veja esta discordância na Figura 32 seguinte:

Em 1900, **Max Planck** revisou a lei de **Rayleigh-Jeans**, obtendo uma lei um tanto diferente. Posteriormente, uma derivação mais completa, a qual incluía uma constante de proporcionalidade, foi apresentada por **Rayleigh-Jeans** em 1905.

## 1.24 Bibliografia e Fonte de Consulta

Ronan, Colin A. (1987). História Ilustrada da Ciência. Universidade de Cambridge. III - Da Renascença à Revolução Científica 1 ed. São Paulo: Círculo do Livro.

Henry, John, (1998). A Revolução Científica e as Origens da Ciência Moderna 1 ed. [S.l.: s.n.] ISBN 9788571104426



Figura 31 – James Jeans - Ajudou a descobrir a lei de Rayleigh-Jeans.

Fonte: <[https://pt.wikipedia.org/wiki/James\\_Hopwood\\_Jeans](https://pt.wikipedia.org/wiki/James_Hopwood_Jeans)>

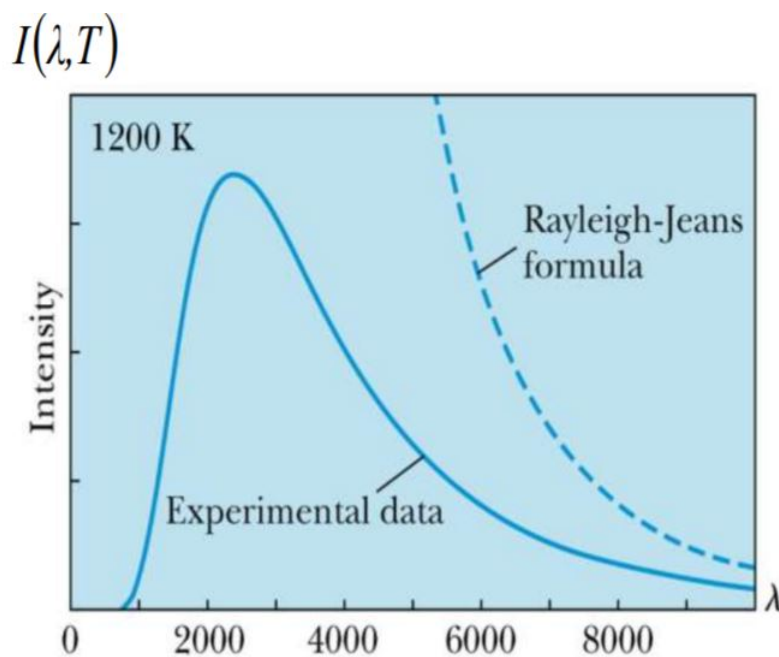


Figura 32 – Fórmula de Rayleigh-Jeans mostrando a catástrofe ultravioleta quanto a distribuição espectral de um corpo negro.

Fonte: <[http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo\\_negro.pdf](http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo_negro.pdf)>

Limite Quântico x Limite Clássico - <<https://otelhado.wordpress.com/2010/08/16/o-que-define-algo-como-...>>



Classical limit of quantum mechanics - <[www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1806-11172003000200006](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1806-11172003000200006)>

Limite Clássico da mecânica quântica - Revista Brasileira de Ensino - <[www.ebah.com.br/content/ABAAAUTEAE/limite-classico-mecanica-quantica](http://www.ebah.com.br/content/ABAAAUTEAE/limite-classico-mecanica-quantica)>

Constante de Planck - <[http://www.ifsc.usp.br/~lavfis/images/.../CtePlanck\\_1.pdf](http://www.ifsc.usp.br/~lavfis/images/.../CtePlanck_1.pdf)>

Computação Quântica - <[https://pt.wikipedia.org/wiki/Computacao\\_quantica](https://pt.wikipedia.org/wiki/Computacao_quantica)>

Constante de Planck: Uma Nova Visao para o Ensino Medio - <[http://qnesc.sbq.org.br/online/qnesc33\\_4/246-EEQ-6011.pdf](http://qnesc.sbq.org.br/online/qnesc33_4/246-EEQ-6011.pdf)>

História da mecânica quântica - <[https://pt.wikipedia.org/wiki/Historia\\_da\\_mecanica\\_quantica](https://pt.wikipedia.org/wiki/Historia_da_mecanica_quantica)>

Max Planck: the reluctant revolutionary - <<http://physicsworld.com/cws/article/print/2000/dec/01/max-planck-the-reluctant-revolutionary>>

Teoria de Max Planck - <<http://brasilecola.uol.com.br/quimica/teoria-max-planck.htm>>

## 1.25 Referências e Leitura Recomendada

A. Hermann: *Lexikon - Geschichte der Physik A-Z* (1978). Aulis-Verlag Deubner & Co KG.

J. Branson: *Quantum Physics 130A* (2001). lecture notes, <[http://heppc16.ucsd.edu/ph130a/130a\\_notes/node15.html](http://heppc16.ucsd.edu/ph130a/130a_notes/node15.html)>.

D.C. Cassidy: *Exhibit on Werner Heisenberg* (1998). American Institute of Physics, <[http://www.aip.org/history/heisenberg/p09\\_text.htm](http://www.aip.org/history/heisenberg/p09_text.htm)>.

A. Einstein, B. Podolsky, N. Rosen: *Can quantum-mechanical description of physical reality be considered complete?* (1935). Physical Review 47, pp. 777-780.

R. Solovay and V. Strassen: *A Fast Monte-Carlo Test for Primality* (1977). SIAM Journal on Computing, 1977, pp. 84-85.

M.A. Nielsen and I.L. Chuang: *Quantum Computation and Quantum Information* (2000). Cambridge University Press.

M. Agrawal, N. Kayal, N. Saxena: *PRIMES is in P* (2002). preprint, <<http://www.cse.iitk.ac.in/users/manindra/primality.ps>>.

D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer* (1985). Proc. R. Soc., London, A 400, pp.97-117.

K. Svozil: *Quantum algorithmic information theory* (1996). Journal of Universal Computer Science 2, pp. 311-346

D. Deutsch and R. Jozsa: *Rapid solution of problems by quantum computer* (1992). Proc. Roy. Soc. London, Ser. A, vol. 439, pp.553-558.

R. P. Feynman: *Quantum mechanical computers* (1985). Optics News 11, pp 11-20.

P. W. Shor: *Algorithms for quantum computation: Discrete logarithms and factoring* (1994). Proceeding. 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA.

Lov K. Grover: *A fast quantum mechanical algorithm for database search* (1996). Proceeding of the 28th Annual ACM Symposium on Theory of Computing.

J. I. Cirac, P. Zoller: *Quantum Computations with Cold trapped Ions* (1995). Phys. Rev. Lett. 74, p. 4091.

I. L. Chuang et al.: *NMR quantum computing: Realizing Shor's algorithm* (2001). Nature 414, pp. 883-887.



# O Século da Física Quântica

A partir do final do século XIX e início do século XX, diversos fenômenos desafiavam a capacidade de explicação das teorias físicas vigentes. A grande revolução científica no século XX teve início, a partir de uma crise que a Física atravessava no fim do século XIX, pois neste período haviam alguns fenômenos naturais que não eram explicados pelas teorias físicas até então existentes. No início do século XX, a Física clássica enfrentava dificuldades em descrever alguns fenômenos observados à época. Dentre esses fenômenos, pode-se citar a (a) radiação de corpo negro, (b) o efeito fotoelétrico, (c) as características ondulatórias do elétron em experimento de dupla fenda e o experimento de **Stern-Gerlach**.

A mecânica quântica é produto das tentativas de se explicar esses fenômenos de modo compatível com o que se observa experimentalmente. Nesse escopo, existe uma data precisa para o nascimento da Física Quântica. Trata-se do dia 14 de dezembro de 1900, quando o cientista **Planck** explica a emissão de radiação do *corpo negro*. Essa crise culminou na criação da mecânica quântica, que se consolidou por volta da década de 1920, e tem sido aplicada com sucesso em diversos fenômenos ([NIELSEN; CHUANG, 2010](#))(p.2). Após os primeiros indícios da revolução quântica que viria acontecer, este capítulo focaliza os resultados mais relevantes no desenvolvimento da Física Quântica no século XX, que redundaram no surgimento da Teoria Quântica. A posterior realização do clássico *experimento da fenda dupla* com elétrons demonstrou que também as partículas poderiam apresentar *comportamento ondulatório*. Não apenas o que sempre fora tido como *onda*, poderia apresentar comportamento de partícula como a luz, mas entidades classicamente consideradas partículas poderiam ter comportamento de onda como os elétrons.

## 2.1 A emissão de radiação do corpo negro

Na Física, um *corpo negro* é aquele que absorve toda a radiação eletromagnética que nele incide; nenhuma luz nele o atravessa e nem é refletida. Um corpo com essa propriedade, em princípio, não pode ser visto, daí o nome *corpo negro*. A explicação elaborada por **Planck** foi baseada na hipótese de que a radiação deveria ser quantizada. Um "corpo negro" é o nome que se dá para um corpo perfeitamente escuro, que absorva qualquer radiação que incida sobre ele. Sabemos que corpos aquecidos acima do zero absoluto radiam calor de volta para o ambiente. Podemos prever

qual vai ser o espectro de emissão de um corpo em equilíbrio térmico baseando-nos nas leis da Física clássica. Ao tentar estudar o problema do emissor ideal (o tal corpo negro) em equilíbrio térmico, chegou-se a um impasse: a Física clássica previa que ele deveria emitir uma quantidade infinita de radiação, porque todos os modos de vibração do campo eletromagnético contínuo tinham que ter a mesma energia. E como a teoria previa um espectro contínuo infinito, a energia emitida devia ser infinita também (STEIN, 2008).

Em fins do século XIX, uma das dificuldades da Física consistia na interpretação das leis que governam a emissão de radiação por parte dos corpos negros. Tais corpos são dotados de alto coeficiente de absorção de radiações. Por isso, parecem negros para a visão humana. Em 1899, após pesquisar as radiações eletromagnéticas, descobriu-se uma nova constante fundamental, batizada posteriormente em sua homenagem como *Constante de Planck*. Um ano depois, **Planck** descobriu a lei da radiação térmica, chamada *Lei de Planck da Radiação*. Essa foi a base da *teoria quântica*, que surgiu dez anos depois com a colaboração de **Albert Einstein** e **Niels Bohr**.



Figura 33 – Mark Planck - Explicou a emissão de radiação do corpo negro.

Fonte: <[https://en.wikipedia.org/wiki/Mark\\_plank](https://en.wikipedia.org/wiki/Mark_plank)>

## 2.2 Marx Planck - 1900

**Marx Karl Ernst Ludwig Planck** (1858-1947) foi um físico alemão. É neste cenário de descobertas e de dúvidas que, o físico alemão **Marx Planck** (1858-1947) introduziu a ideia de que a energia é uma grandeza discreta (o conceito de energia quantizada) (WIKIPEDIA, 1999). Ao contrário dos preceitos da Física clássica, sua sugestão foi que a energia ocorria em pequenas porções, chamadas de *quanta* (plural de *quantum*). Atualmente um *quantum* é chamado de *fóton* <<http://brasilecola.uol.com.br/quimica/teoria-max-planck.htm>>.

Dentro deste contexto, admitindo-se que um átomo vibre com uma frequência  $v$ , quer seja para dar origem às raias espectrais da lâmpada de hidrogênio, ou à emissão de um corpo negro, a energia associada  $E$  pode existir apenas em quantidades muito bem definidas  $E = hv$ , onde  $h$  é a constante de **Planck** ( $6.62 \times 10^{-34} Js$ ), como em <<https://physics.aps.org/story/v3/st23>>. Ao trabalho de **Planck** seguiram outras importantes contribuições que deram origem à chamada Física Quântica.

Ambas as deficiências (radiação dos corpos negros e o espectro de energia discreta de átomos), se revelariam cruciais no desenvolvimento da teoria quântica. A expressão **teoria quântica** tem origem no termo latino *quantum*, que significa *unidade mínima, indivisível*. Foi utilizada por **Max Planck** em 1900, no trabalho que deu início ao desenvolvimento da mecânica quântica.



Figura 34 – Marx Planck - introduziu o conceito de energia quantizada.

Fonte: <<http://brasilecola.uol.com.br/quimica/teoria-max-planck.htm>>

Era 14 de Dezembro de 1900. Numa reunião, **Max Planck** apresentou seu artigo "*Sobre a Teoria da Lei de Distribuição de Energia do Espectro Normal*". Isso foi o início de uma revolução na Física - a Física Quântica! Assim como a Teoria da Relatividade, a Física Quântica representa uma generalização da Física clássica (a velocidade da luz, como constante universal). A Teoria da Relatividade estende as leis físicas para a região de grandes velocidades. A Física Quântica estende esse campo à regiões de dimensões microscópicas. A *constante de Planck* caracteriza a física quântica.

No contexto do bem-sucedido desenvolvimento da Mecânica Clássica, do *Eletromagnetismo* e da *Termodinâmica*, os físicos do início do século XX buscavam solucionar questões cruciais que estavam na fronteira da ciência da época. O interesse predominante se concentrava na obtenção de um modelo definitivo para o átomo e na explicação dos fenômenos relacionados à natureza da luz. A efervescência da busca pelas respostas corretas fez com que o primeiro quarto do século passado fosse

marcado pelo nascimento de um dos maiores triunfos científicos de todos os tempos: a *física quântica*.

Um dos principais problemas de então consistia em **explicar a maneira pela qual a energia da radiação térmica se distribuía ao longo das diversas frequências do espectro eletromagnético**. A dificuldade foi resolvida em 1900, quando o físico alemão **Max Planck** (1858-1947) assumiu que **a energia era liberada de modo discreto, e não contínuo**, na forma de vários pequenos "pacotes" com energia proporcional à frequência da radiação - aos quais ele denominou *quanta*, plural da palavra latina *quantum*. No início do século XX, ao tentar explicar, matematicamente, a radiação de corpo negro, **Max Planck** introduziu o conceito de *quantum de energia*.

### 2.2.1 Planck resolveu o problema

Foi **Planck** quem resolveu o problema 35:

- A resposta a esse problema foi dada por **Max Planck** em 1900. **Planck** percebeu que o problema poderia ser resolvido, se os objetos radiantes (átomos) só pudessem emitir (ou absorver) energia em determinadas quantidades fixas, que ele chamou de **quanta** (plural de quantum).
- A teoria de **Planck** resolveu o problema. Objetos frios não tem energia suficiente para produzir muitos *quanta* de alta frequência. Eles só conseguem irradiar energia na faixa de frequência em que a energia disponível em cada átomo seja comparável à dos *quanta* envolvidos na radiação.
- Ele utilizou a estatística de **Boltzmann** para obter uma equação teórica que concordava com os resultados experimentais para todos os comprimentos de onda.
- **Planck** utilizou apenas um artifício para resolver o problema! Mas sem embaçamento físico !

Há 118 anos, quando **Max Planck** publicou o artigo que deu origem à mecânica quântica, a história continua. A história revela, no entanto, que **Planck** não percebeu imediatamente as consequências de seu trabalho e, se tornou revolucionário contra sua vontade ([WORLD, 2000](#)). Há 100 anos atrás, **Planck** foi o prêmio Nobel de Física em 1918. Planck ficou considerado o pai da Física Quântica e um dos físicos mais importantes do século XX.

### 2.2.2 A ideia da quântica: energia existente apenas em certos níveis

Certo dia, em 1900, o físico **Mark Planck** (1858-1947) fez uma suposição bizarra, numa tentativa de escapar à *catástrofe ultravioleta*. Em vez de supor que a energia poderia ser irradiada em qualquer frequência, ele presumiu que apenas um número finito de frequências era possível, e estes eram todos múltiplos de uma frequência mínima. Em analogia com a velocidade de um carro, a hipótese de **Planck** seria de que, por exemplo, somente velocidades que fossem múltiplas de 5, como 15 Km/h, 35 Km/h, 60 Km/h, entre outras, seriam possíveis. Ele conseguiu mostrar quase imediatamente que essa hipótese contra-intuitiva resolveria o problema. E as curvas de radiação que ele obteve ao fazer essas suposição corresponderiam àquelas

Lei da Radiação de Planck

$$I = \frac{2\pi c^2 h}{\lambda^5} \frac{1}{e^{hc/\lambda kT} - 1}$$

Planck fez duas modificações na teoria clássica:

- Os osciladores (de origem electromagnética) podem ter apenas certas energias discretas:

$$E_n = nhf$$

onde  $n$  é um número inteiro,  $f$  é a frequência, e  $h$  é chamada de constante de Planck:

$$h = 6.6261 \times 10^{-34} \text{ J.s}$$

- Os osciladores podem absorver ou emitir energia em múltiplos discretos de um quantum fundamental de energia dada por:

$$\Delta E = hf$$

Figura 35 – A Lei da Radiação de Planck.

Fonte: <[http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo\\_negro.pdf](http://professor.ufabc.edu.br/~joseantonio.souza/wp-content/uploads/2016/07/Aula-8-Corpo_negro.pdf)>

registradas experimentalmente. Naquele dia, enquanto caminhava com seu filho pequeno depois do almoço, ele disse:

"Hoje, tive uma ideia tão revolucionária e grandiosa quanto aquela de **Newton**."

Outros físicos, seus colegas, de início, não viram a ideia de **Planck** dessa maneira. **Planck** era um físico respeitado, mas a ideia da Quântica - energia existente apenas em certos níveis - não foi, a princípio, levada a sério. Foi vista como uma espécie de truque matemático que resolvia a *catástrofe ultravioleta*, mas o fazia recorrendo a regras às quais o mundo real não obedecia.

De 1905 a 1909, **Planck** atuou como diretor-chefe da *Deutsche Physikalische Gesellschaft* (Sociedade Alemã de Física). Em 1913, foi nomeado reitor da Universidade de Berlim. **Planck** foi laureado com o Nobel de Física de 1918 ([PRIZE, 2014](#)), por suas contribuições na área da Física Quântica.

## 2.3 Einstein e o efeito fotoelétrico - 1905

A deia de **Mark Planck** se arrastou por cinco anos, até que **Albert Einstein** (1879-1955) a usou em 1905, para explicar o *efeito fotoelétrico*, que era outro fenômeno não explicado pela teoria ondulatória da luz. O *efeito fotoelétrico consiste na emissão de elétrons por uma superfície metálica bombardeada por um feixe de luz*. Embora muitos de nós não saibamos, tal efeito é bem familiar, pois está presente em nosso cotidiano, como por exemplo, como era o funcionamento dos tubos de raios catódicos (em televisão e vídeos em computadores mais antigos), as portas que abrem e fecham automaticamente, e um exemplo mais moderno, a geração energia elétrica através de



placas fotovoltaicas a partir da luz do sol, que têm o funcionamento baseado nesse fenômeno. **Einstein** explicou o efeito fotoelétrico admitindo a hipótese de que a luz é constituída por pacotes concentrados de energia, que atualmente denominamos *fótons*, e assim, o fenômeno em questão é facilmente explicado quando consideramos a colisão entre os *fótons* da radiação incidente e os elétrons dos metais.

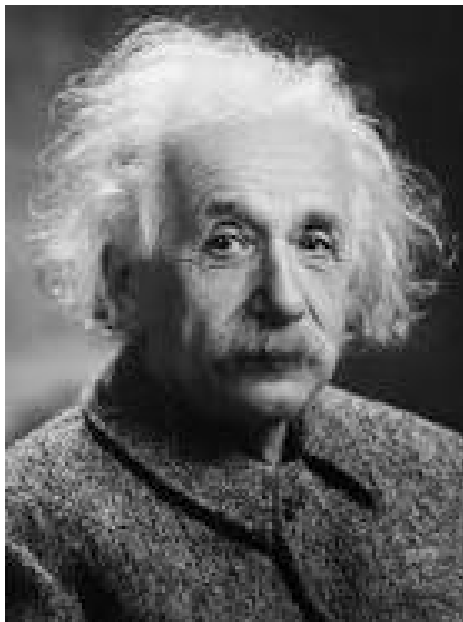


Figura 36 – Albert Einstein - Prêmio Nobel de Física de 1921, por suas contribuições à física teórica e, especialmente, por sua descoberta da lei do efeito fotoelétrico, que foi fundamental no estabelecimento da teoria quântica.

Fonte: <[https://en.wikipedia.org/wiki/Albert\\_Einstein](https://en.wikipedia.org/wiki/Albert_Einstein)>

É importante notarmos que os trabalhos de **Einstein** e **Planck** sugeriam a *quantização*, mas não explicavam o porquê. A hipótese se mostrou capaz de explicar matematicamente a distribuição de energia, e foi o passo primordial de todo o desenvolvimento subsequente.

**Einstein** explicou o *efeito fotoelétrico* postulando a existência de partículas leves, mais tarde chamados **fótons**, com a energia  $E = h\nu$

Em 1905, **Albert Einstein** apresentou, também, sob a forma de cinco artigos, as base da *Relatividade* e da *mecânica quântica*. Tais "*fenômenos rebeldes*" finalmente foram explicados. Embora à época não fosse admitida outra forma de propagação da luz, senão a ondulatória, intrigava a existência de um fenômeno cujo mecanismo não podia ser explicado em termos da luz enquanto *onda*.

Verificava-se, então, o chamado *efeito fotoelétrico* quando uma placa metálica era bombardeada por um feixe luz e tinha elétrons arrancados de sua superfície. **Einstein** explicou o efeito a partir de uma mudança fundamental de paradigma: segundo ele, a própria luz era constituída de *quanta*, e eram essas partículas de luz, mais tarde denominadas *fótons*, que interagem com os elétrons do metal individualmente. Descobria-se, assim, a *dualidade onda-partícula* da radiação eletromagnética: **dependendo do experimento, a natureza da luz poderia ser percebida como ondulatória ou corpuscular.**

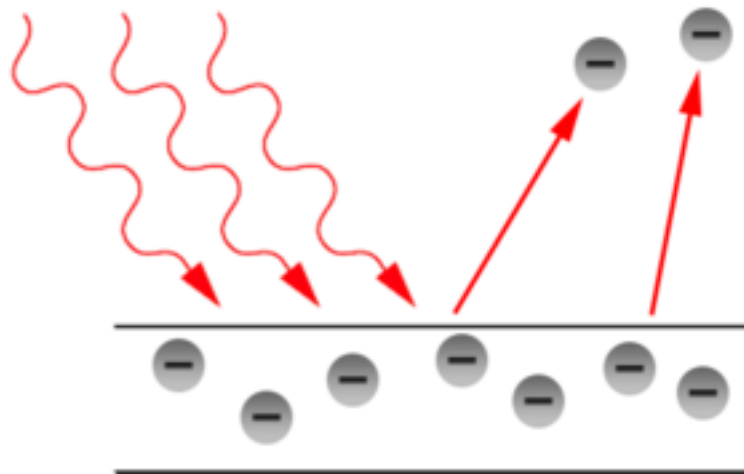


Figura 37 – Einstein - O efeito fotoelétrico, a emissão de elétrons por um material, geralmente metálico, quando exposto a uma radiação eletromagnética (como a luz) de frequência suficientemente alta, que depende do material, causa a placa perder elétrons.

Fonte: <[https://pt.wikipedia.org/wiki/Efeito\\_fotoeletrico](https://pt.wikipedia.org/wiki/Efeito_fotoeletrico)>

## 2.4 O modelo atômico de Rutherford - 1911

No ano de 1911, **Ernest Rutherford** (1871-1937), um físico e químico neozelandês naturalizado britânico, se tornou conhecido como o pai da física nuclear. Foi premiado com o Nobel de Química em 1908, por suas investigações sobre a desintegração dos elementos e a química das substâncias radioativas. Ele defendeu que os átomos têm sua carga positiva concentrada em um pequeno núcleo, e, desse modo, foi criado o modelo atômico de **Rutherford**. Ele propôs um modelo atômico no qual os elétrons circulavam o núcleo de carga positiva. Embora fosse simples e coerente, esse modelo apresentava um erro incorrigível, pois toda partícula que descreve um movimento circular possui *aceleração*. Dessa forma, como havia explicado **Maxwell**, através de suas equações, *por ter aceleração o elétron deveria emitir luz*, perdendo energia gradualmente até se chocar com o núcleo.

## 2.5 Niels Bohr: um novo modelo de átomo adotando uma abordagem quântica - 1913

Em 1913, oito anos mais tarde de **Einstein** e dois anos apenas de **Rutherford**, **Niels Henrik David Bohr** (1885-1962), um físico dinamarquês cujos trabalhos contribuíram decisivamente para a compreensão da estrutura atômica e da Física Quântica, a utilizou para explicar o espectro do átomo do hidrogênio. Dezoito anos mais tarde (1918), **Planck** ganharia o *Prêmio Nobel de Física* e **Bohr** receberia o Nobel de Física em 1922, e a mecânica quântica se tornaria uma das teorias fundamentais da Física, explicando o comportamento do mundo dos átomos e



Figura 38 – Ernest Rutherford - O pai da física nuclear: a desintegração dos elementos e a química das substâncias radioativas.

Fonte: <[https://pt.wikipedia.org/wiki/Ernest\\_Rutherford](https://pt.wikipedia.org/wiki/Ernest_Rutherford)>

tornando possíveis muitas das indústrias de alta tecnologia dos dias de hoje.

Na época, era ainda misteriosa a origem do tipo de luz emitida por gases aquecidos. Sabia-se que o espectro resultante era discreto, com emissão de radiação apenas em certas frequências. A causa, porém, era completamente desconhecida. A solução do enigma foi dada por **Niels Bohr** (1885-1962), que desenvolveu um novo modelo de átomo adotando uma abordagem quântica. Segundo **Bohr**, os elétrons orbitavam o núcleo atômico e podiam ocupar apenas certas órbitas, caracterizadas por quantidades específicas de energia. Os elétrons podiam ainda saltar de uma órbita a outra conforme perdessem ou ganhassem energia, liberando ou absorvendo um fóton de energia equivalente. O modelo se mostrou extremamente adequado para explicar a estranha emissão: aquecendo-se um gás, os elétrons de seus átomos ganhavam energia e realizavam um salto quântico para uma órbita superior; no salto de retorno à órbita original, liberavam um *fóton* com energia igual à inicialmente recebida. **Niels Bohr**, baseando-se nos conceitos de quantização, estipulou que a energia dos elétrons em suas órbitas em torno do núcleo também era quantizada. Isto é, em um átomo como o do hidrogênio existem várias órbitas estáveis possíveis para o elétron, cada uma com energia diferente. Assim, ele pôde corrigir o modelo de **Rutherford**.

Em 1913, **Niels Bohr** calculou o valor da *constante de Rydberg*, assumindo que o momento angular de elétrons que orbitam o núcleo satisfaz a condição de quantização  $L = n.h/2\pi$ . Essa restrição poderia ser justificada atribuindo-se propriedades da onda ao elétron e exigindo que suas *funções de onda* correspondentes formassem uma *onda* estável; no entanto, esse tipo da teoria híbrida permaneceu insatisfatória.



Figura 39 – Niels Bohr - Contribuiu decisivamente para a compreensão da estrutura atômica e da Física Quântica.

Fonte: <[https://pt.wikipedia.org/wiki/Niels\\_Bohr](https://pt.wikipedia.org/wiki/Niels_Bohr)>

Com a ascensão do nazismo (nacional-socialismo, mais comumente conhecido como nazismo, é a ideologia associada ao Partido Nazista, ao Estado nazista), a ciência alemã sofreu severamente. Muitos dos cientistas de ponta eram judeus ou tinham parentes judeus, e fugiram do país. Muitos outros reagiram com horror ao regime nazista, e também partiram. **Planck**, embora condenando os nazistas, resolveu ficar na Alemanha. Essa se revelaria uma escolha trágica. Em 1945, o filho mais novo de **Planck** foi executado por sua participação numa revolta, uma tentativa fracassada para assassinar Hitler.

## 2.6 A contribuição de Schrödinger - 1925

Na mecânica quântica, a *equação de Schrödinger* é uma equação diferencial parcial que descreve como o estado quântico de um sistema físico muda com o tempo. Foi formulada no final de 1925, e publicada em 1926, pelo físico austríaco **Erwin Rudolf Josef Alexander Schrödinger** (1887-1961).

Com o trabalho de **Schrödinger** e **Werner Karl Heisenberg** (1901-1976), em 1925, é que a teoria quântica se estabeleceu. **Schrödinger** foi um físico teórico austríaco, conhecido por suas contribuições à mecânica quântica, especialmente a *equação de Schrödinger*. Ele postulou uma equação que permite calcular os níveis de energia e a probabilidade de se encontrar uma partícula em determinada região.

Em janeiro de 1926, ele publicou no *Annalen der Physik* o trabalho "*Quantisierung als Eigenwertproblem*" (*Quantização como um Problema de Autovalor*) em mecânica de ondas e que hoje é conhecido como a *equação de Schrödinger*. Este trabalho tem sido universalmente considerado como uma das conquistas mais importantes

do século XX, criando uma revolução na mecânica quântica. Ver no capítulo seguinte em 2.6. Neste trabalho ele deu uma "derivação" da equação de onda para sistemas independentes de tempo, e mostrou que fornecia autovalores de energia corretos para o átomo de hidrogênio. Este trabalho tem sido universalmente considerado como uma das conquistas mais importantes do século XX, criando uma revolução na mecânica quântica, e na verdade em toda a Física e a Química. Um segundo documento foi apresentado, que resolveu o oscilador harmônico quântico e a molécula diatômica, e dá uma nova derivação da *equação de Schrödinger*. Um terceiro documento mostrou a equivalência da sua abordagem à de **Heisenberg**. Um quarto trabalho de sua série mais marcante mostrou como tratar os problemas nos quais o sistema muda com o tempo, como nos problemas de *dispersão*. Estes trabalhos foram os principais de sua carreira e foram imediatamente reconhecidos como tendo grande importância pela comunidade científica. A Teoria Quântica, por sua vez, calcula a probabilidade de se encontrar o elétron (ou outra partícula) em uma região do espaço, usando a equação de **Schrödinger**.

Na mecânica clássica, a equação de movimento é a segunda lei de **Newton** ( $F = m.a$ ) utilizada para prever matematicamente o que o sistema fará a qualquer momento após as condições iniciais do sistema. Na mecânica quântica, o análogo da segunda lei de **Newton** é a *equação de Schrödinger* para o sistema quântico (geralmente átomos, moléculas e partículas subatômicas sejam elas livres, ligadas ou localizadas). Não é uma equação algébrica simples, mas, em geral, uma equação diferencial parcial linear, que descreve o tempo de evolução da *função de onda* do sistema (também chamada de "função de estado"). (GRIFFITHS, 2004)

Usando a notação de **Dirac** (1902-1984), o vetor de estados  $\vec{r}$  é dado, em um instante  $t$ , por  $|\psi(\vec{r}, t)\rangle$ <sup>1</sup>.

A equação de **Schrödinger** dependente do tempo, então, escreve-se:

$$\hat{H} |\psi(\vec{r}, t)\rangle = i\hbar \frac{\partial}{\partial t} |\psi(\vec{r}, t)\rangle$$

Figura 40 – Equação de Schrödinger dependente do tempo.

Fonte: <<https://pt.wikipedia.org/wiki/Equaça~odeSchrödinger>>

Em que  $i$  é a unidade imaginária em  $\mathbb{C}$ ,  $\hbar$  é a constante de **Planck** dividida por  $2\pi$ , e o *Hamiltoniano*  $\hat{H}$  é um operador auto-adjunto atuando no *vetor de estados*  $\vec{r}$ . Em mecânica quântica, o *Hamiltoniano*  $H$  é o observável correspondente à energia total do sistema. Como todos os observáveis, o *espectro do Hamiltoniano* é o conjunto de possíveis resultados quando mede-se a energia total de um sistema.

O conceito de uma *função de onda* é um postulado fundamental da mecânica quântica. A **equação de Schrödinger** também é muitas vezes apresentada como um postulado separado, mas alguns autores (BALLENTINE, 1998), afirmam que pode ser derivada de princípios de *simetria* (Teoria dos Grupos). Geralmente, "derivações" da equação demonstrando sua plausibilidade matemática para descrever

<sup>1</sup> Um vetor  $|\cdot\rangle$  é chamado *ket* (em contraponto com  $\langle\cdot|$ , que será definido posteriormente, e será chamado *bra*).

*dualidade partícula-onda.*

Na interpretação padrão da mecânica quântica, a *função de onda* é a descrição mais completa que pode ser dada a um sistema físico. As soluções para a equação de **Schrödinger** descrevem não só sistemas moleculares, atômicas e subatômicas, mas também os sistemas macroscópicos, possivelmente, até mesmo todo o universo (LALOE, 2012). A equação de **Schrödinger**, em sua forma mais geral, é compatível, tanto com a mecânica clássica, mas a formulação original do próprio **Schrödinger** era não-relativista.

A equação de **Schrödinger** não é a única maneira de fazer previsões em mecânica quântica - outras formulações podem ser utilizadas, tais como a mecânica matricial de **Werner Heisenberg** (uma formulação da mecânica quântica criada por **Werner Heisenberg**, **Max Born**, e **Pascual Jordan** em 1925. Foi a primeira definição completa e correta da mecânica quântica. Ela estendeu o modelo de **Bohr**), e o trajeto da integração funcional (uma integração de funcionais sobre espaços funcionais) de **Richard Feynman**.

## 2.7 Princípio da Incerteza de Heisenberg - 1927

Um resultado importante da mecânica quântica é o chamado *princípio da incerteza*, formulado em 1926 e publicado em 1927 pelo físico alemão **Werner Heisenberg** (1902-1976). O princípio estabelece que é impossível medir simultaneamente a posição e a velocidade de uma partícula com uma precisão melhor do que um número dado por  $h/4\pi$ , onde  $h$  é a constante de Planck <sup>2</sup>. Se tentarmos medir a velocidade e uma partícula com grande precisão, perdemos informação sobre sua localização (posição). Por outro lado, podemos nos fixar na posição, mas aí a incerteza no valor da velocidade aumenta, pois perdemos informação sobre sua velocidade.

Isso pode ser interpretado de uma forma simples como a afirmação de que uma medida inevitavelmente perturba o sistema sendo observado. Em um sentido mais amplo, a razão pela qual não podemos medir posição e velocidade ao mesmo tempo com uma precisão arbitrária é que o conceito de posição e velocidade não existem ao mesmo tempo. Nossa experiência com sistemas clássicos nos leva a acreditar que um fenômeno microscópico pode ser descrito em termos de conceitos tais como posição e velocidade, que surgiram com a observação do movimento de objetos macroscópicos.

O princípio da incerteza leva a efeitos drásticos na escala atômica, mas que não são percebidos na vida cotidiana, pois são muito pequenos. Descobriu-se depois que o *princípio da incerteza* podia ser obtido diretamente a partir da equação de **Schrödinger**, junto com o postulado de **Bohr**.

O *princípio da incerteza* e a ideia de que a função de onda  $\psi$  representava todo nosso conhecimento sobre um sistema foi desenvolvido por **Niels Bohr** em uma nova filosofia da Física que ficou conhecida com *interpretação de Copenhagen*. Segundo **Bohr**, não faz sentido perguntar onde está localizado uma elétron na realidade. Para ele, a única realidade da qual podemos falar é aquela resultante de um processo de medida <sup>3</sup>

<sup>2</sup> Homenagem ao físico alemão **Max Planck** (1847-1947), pioneiro nos estudos da teoria quântica.

<sup>3</sup> O físico russo, naturalizado americano, **George Gamow** (1904-1968) que ficou conhecido pelos seus vários livros de divulgação, contava que **Bohr**, apesar de muito inteligente, tinha o raciocínio

A *interpretação de Copenhague* descreve o que acontece quando um observador faz uma medida, mas o observador e o ato de medir são tratados classicamente.<sup>4</sup> Da mesma forma que existe uma relação de incerteza entre velocidade e posição, como explicado acima, existe outra entre energia e tempo dada por:

$$\Delta E \cdot \Delta t \geq h/4\pi$$

Essa é a relação importante quando analisamos partículas virtuais: como eles existem por um tempo curto, podem fazer "surgir" energia, desde que obedeçam ao princípio da incerteza.

Em 1927, **Heisenberg** formulou o *princípio da incerteza*, que formalizou a *complementaridade da onda* e a *imagem de partículas*, reivindicada por **Bohr** que, embora mutuamente exclusivo, são ambos essenciais para uma completa descrição de eventos quânticos.

O princípio da incerteza, de **Heisenberg** é relativamente simples de ser enunciado e tem uma ideia simples. Na física tradicional newtoniana, também chamada de Física clássica, acreditava-se que se soubermos a posição inicial e o momento (massa e velocidade) de todas as partículas de um sistema, seríamos capaz de calcular suas interações e prever como ele se comportará. Isto parece correto, se soubermos descrever com precisão as interações entre essas partículas, mas parte de um pressuposto bastante forte: o de que, de fato, conhecemos a posição e o momento de todas as partículas.

Segundo o **princípio da incerteza**, não se pode conhecer com precisão absoluta, a *posição* ou o *momento* (e, portanto, a velocidade) de uma partícula. Isto acontece porque para medir qualquer um desses valores acabamos os alterando, e isto não é uma questão de medição, mas sim de física quântica e da natureza das partículas. O princípio da incerteza é equacionado através da fórmula:

$$\Delta x \Delta p \geq \frac{h}{2}$$

No seu nível mais fundamental, o *princípio da incerteza* é uma consequência da  **dualidade partícula-onda** e do **princípio de Broglie**. Se uma partícula encontra-se em uma região com erro  $\Delta x$ , então seu comprimento de onda natural deve ser menor que  $\Delta x$ , o que requer um *momento* elevado, variando entre  $\frac{-h}{\Delta x}$  e  $\frac{+h}{\Delta x}$ . *Aí está a incerteza!* O raciocínio é análogo para a indeterminação do *momento*. **Heisenberg** recebeu o Nobel de Física de 1932, "pela criação da mecânica quântica, cujas aplicações levaram à descoberta, entre outras, das formas alotrópicas do hidrogênio".

---

lento. Ele gostava de filmes de faroeste, mas ninguém queria acompanhá-lo ao cinema, porque ele custava a entender o enredo e ficava fazendo perguntas o tempo todo, para desagrado dos demais expectadores. Quando ele assistia uma palestra, custava a entender o que o palestrante estava dizendo. Todos começavam a explicar a **Bohr** o que ele não havia entendido e, no final, ele acabava por entender mais do problema do que os outros, inclusive o próprio palestrante. Famosas são as objeções que **Einstein** levantava contra a mecânica quântica e que eram, depois de algum tempo, respondidas por **Bohr**.

<sup>4</sup> O físico norte-americano **Steven Weinberg** (1933-) dizia que isso estava errado: os físicos e seus equipamentos deveriam ser governados pelas mesmas regras quânticas que governam o Universo como um todo.

**Schrödinger** recebeu o Nobel de Física em 1933.

Eles colocaram a base teórica da mecânica quântica, para a *Interpretação de Copenhague* (CASSIDY, 1998).

" *We regard quantum mechanics as a complete theory for which the fundamental physical and mathematical hypotheses are no longer susceptible of modification.*"

Werner Heisenberg and Max Born, Solvay Congress of 1927.

Na década de 1920, as interpretações do comportamento ondulatório da matéria e o formalismo matemático desenvolvido conduziram a uma formulação da mecânica adequada ao mundo microscópico, a mecânica quântica, delimitando decisivamente os revolucionários limiares da Física moderna (EISBERG; RESNICK, 1979a) (FEYNMAN, 2008) (HEWITT, 2015). A ontologia determinística estrita, característica da *mecânica newtoniana* - foi abalada seriamente, após a publicação do *Princípio da Incerteza* de **Werner Heisenberg** em 1927, e do *Princípio da Complementaridade* de **Niels Bohr**.

Embora a explicação de fenômenos quânticos como *emaranhamento quântico* ou *medição quântica* ainda parece um pouco insatisfatório, mesmo após 75 anos, a *Interpretação de Copenhague*, ainda pode ser considerada como a corrente filosófica principal em Física quântica. As contradições aparentes como o paradoxo *EPR* (EINSTEIN; PODOLSKY; ROSEN, 1935) não têm apenas sido verificado experimentalmente, mas também servem como princípios fundamentais para novos campos de pesquisa como *criptografia quântica* e *computação quântica*.

## 2.8 Bibliografia e Fonte de Consulta

Ronan, Colin A. (1987). *História Ilustrada da Ciência*. Universidade de Cambridge. III - Da Renascença à Revolução Científica 1 ed. São Paulo: Círculo do Livro.

Henry, John, (1998). *A Revolução Científica e as Origens da Ciência Moderna* 1 ed. [S.l.: s.n.] ISBN 9788571104426.

Bernhard Ömer, *Structured Quantum Programming*, first version, 26th May 2003, last revision, 2nd September 2009, Institute for Theoretical Physics, Vienna University of Technology. <<http://tph.tuwien.ac.at/~oemer/doc/structqprog.pdf>>

A Onda dos Qubits - o conceito de Discórdia Quântica - <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>

O Spin que move o mundo - <[http://www.cienciahoje.org.br/noticia/v/ler/id/2781/n/o\\_spin\\_que\\_move\\_o\\_mundo](http://www.cienciahoje.org.br/noticia/v/ler/id/2781/n/o_spin_que_move_o_mundo)>

Limite Quântico x Limite Clássico - <<https://otelhado.wordpress.com/2010/08/16/o-que-define-algo-como-...>>

Classical limit of quantum mechanics - <[www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1806-11172003000200006](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1806-11172003000200006)>



Limite Clássico da mecânica quântica - Revista Brasileira de Ensino - <[www.ebah.com.br/content/ABAAAUTEAE/limite-classico-mecanica-quantica](http://www.ebah.com.br/content/ABAAAUTEAE/limite-classico-mecanica-quantica)>

Constante de Planck - <[http://www.ifsc.usp.br/~lavfis/images/.../CtePlanck\\_1.pdf](http://www.ifsc.usp.br/~lavfis/images/.../CtePlanck_1.pdf)>

Computação Quântica - <[https://pt.wikipedia.org/wiki/Computacao\\_quantica](https://pt.wikipedia.org/wiki/Computacao_quantica)>

Constante de Planck: Uma Nova Visao para o Ensino Medio - <[http://qnesc.sbq.org.br/online/qnesc33\\_4/246-EEQ-6011.pdf](http://qnesc.sbq.org.br/online/qnesc33_4/246-EEQ-6011.pdf)>

História da Mecânica Quântica - <[https://pt.wikipedia.org/wiki/Historia\\_da\\_mecanica\\_quantica](https://pt.wikipedia.org/wiki/Historia_da_mecanica_quantica)>

Max Planck: the reluctant revolutionary - <<http://physicsworld.com/cws/article/print/2000/dec/01/max-planck-the-reluctant-revolutionary>>

Teoria de Max Planck - <<http://brasilecola.uol.com.br/quimica/teoria-max-planck.htm>>

Átomos de Rydberg - <<https://periodicos.ufsc.br/index.php/fisica/article/viewFile/7937/7303>>, Cad. Cat. Ens. Fis., Florianópolis, 3(1): 41-45, abr. 1986.

## 2.9 Referências e Leitura Recomendada

Ludwig Boltzmann: Ableitung des Stefan'schen Gesetzes, betreffend die Abhängigkeit der Wärmestrahlung von der Temperatur aus der electromagnetischen Lichttheorie. In: Annalen der Physik und Chemie. Band 22, 1884, S. 291-294, doi:10.1002/andp.18842580616.

A. Hermann: *Lexikon - Geschichte der Physik A-Z* (1978). Aulis-Verlag Deubner & Co KG.

J. Branson: *Quantum Physics 130A* (2001). lecture notes, <[http://heppc16.ucsd.edu/ph130a/130a\\_notes/node15.html](http://heppc16.ucsd.edu/ph130a/130a_notes/node15.html)>.

D.C. Cassidy: *Exhibit on Werner Heisenberg* (1998). American Institute of Physics, <[http://www.aip.org/history/heisenberg/p09\\_text.htm](http://www.aip.org/history/heisenberg/p09_text.htm)>.

A. Einstein, B. Podolsky, N. Rosen: *Can quantum-mechanical description of physical reality be considered complete?* (1935). Physical Review 47, pp. 777-780.

R. Solovay and V. Strassen: *A Fast Monte-Carlo Test for Primality* (1977). SIAM Journal on Computing, 1977, pp. 84-85.

M.A. Nielsen and I.L. Chuang: *Quantum Computation and Quantum Information* (2000). Cambridge University Press.

M. Agrawal, N. Kayal, N. Saxena: *PRIMES is in P* (2002). preprint, <<http://www.cse.iitk.ac.in/users/manindra/primality.ps>>.

D. Deutsch: *Quantum theory, the Church-Turing principle and the universal quantum computer* (1985). Proc. R. Soc., London, A 400, pp.97-117.

K. Svozil: *Quantum algorithmic information theory* (1996). Journal of Universal Computer Science 2, pp. 311-346

D. Deutsch and R. Jozsa: *Rapid solution of problems by quantum computer* (1992). Proc. Roy. Soc. London, Ser. A, vol. 439, pp.553-558.

R.P. Feynman: *Quantum mechanical computers* (1985). Optics News 11, pp 11-20.

P.W. Shor: *Algorithms for quantum computation: Discrete logarithms and factoring* (1994). Proceeding. 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA.

Lov K. Grover: *A fast quantum mechanical algorithm for database search* (1996). Proceeding of the 28th Annual ACM Symposium on Theory of Computing.

J.I. Cirac, P. Zoller: *Quantum Computations with Cold trapped Ions* (1995). Phys. Rev. Lett. 74, p. 4091.

I.L. Chuang et al.: *NMR quantum computing: Realizing Shor's algorithm* (2001). Nature 414, pp. 883-887.



## A Revolução Quântica

Uma *teoria* (do grego, 'contemplação', 'reflexão', 'introspecção') indica, na linguagem comum, uma ideia nascida com base em alguma *hipótese*, conjectura ou suposição, mesmo abstrata, sobre uma realidade. Também designa o conhecimento descritivo puramente racional ou a forma de pensar e entender algum fenômeno a partir da observação.

A *Teoria Quântica* também é conhecida como *mecânica quântica* ou *Física Quântica*, e tem como foco principal de estudo, o mundo microscópico. A *Teoria Quântica* deve ser sempre referida destacando-se os trabalhos de **Planck**, **Einstein**, **Rutherford**, **Bohr**, **Schrödinger**, **Dirac** e **Pauli**, entre outros. Os princípios da quantização da energia, propostos por **Einstein** e **Planck**, e as observações experimentais do espectro atômico dos elementos mostravam que as leis de **Newton** não produziam resultados corretos quando aplicadas a sistemas muito pequenos, como átomos e moléculas. Para explicar o movimento dos elétrons em torno do núcleo foi criada - por **Planck**, **Bohr**, **Einstein** e **Schrödinger** - uma nova teoria, a da mecânica quântica. Apesar de seu enorme sucesso, a teoria de **Bohr** tinha várias lacunas. O espectro de átomos mais complexos não podia ser explicado, gerando perguntas como: por que algumas raias do espectro são mais intensas do que outras? E, principalmente, como os átomos interagem uns com os outros formando sistemas estáveis?

### 3.1 A revolução quântica

A ideia revolucionária de **Mark Planck** fez mais do que simplesmente resolver a *catástrofe ultravioleta*. Possivelmente, só outro momento da ciência abriu um portal para um mundo tão inesperado - quando **Anton von Leeuwenhoek** (1632-1723), um cientista e construtor de microscópios holandês, usou seu microscópio primitivo e examinou com ele uma gota de água, para então descobrir formas de vida jamais imaginadas ou vistas até então.

Um problema parecido surgiu quando o físico dinamarquês **Niels Bohr**, em 1913, introduziu o seu modelo atômico, no qual supôs que o *elétron* poderia se mover somente em órbitas determinadas, onde não emitia radiação eletromagnética. A radiação era emitida somente quando o *elétron* passava de uma órbita para outra. Com esse modelo, **Bohr** solucionou a estabilidade atômica e explicou o espectro

discreto de radiação para o átomo de hidrogênio, porém, não ficou claro o motivo pelo qual o *elétron* não poderia ocupar posições intermediárias no espaço.

Assim, por meio desses exemplos, percebemos que a teoria quântica desenvolvida até o primeiro quarto do século XX possuía bases teóricas e conceituais frágeis (com uma rosa, as teorias eram frágeis, mas não fracas), pois os princípios eram esparsos e os enunciados eram criados com a finalidade específica de atender a uma necessidade (ou problema) pontual. Nesse escopo, os físicos ressentiam-se de postulados autênticos e princípios gerais dos quais poderiam formular uma teoria consistente, eficiente e abrangente. Esse desejo dos físicos se tornou realidade com o surgimento da mecânica quântica (PIRES; CARVALHO, 2014) (GRIFFITHS, 2004).

A revolução quântica mudou nosso mundo - tecnológica, científica e filosoficamente. Boa parte da incrível tecnologia que foi desenvolvida desde a década de 1930 - o computador, os *scanners* médicos, os *lasers*, todas as coisas com um chip dentro - resulta da aplicação da teoria quântica à compreensão do comportamento do mundo subatômico. A mecânica quântica não apenas gerou ciências que não existiam antes dela, mas também enriqueceu imensamente algumas das mais veneráveis áreas de estudo, como a Química e a Física. Por fim, a mecânica quântica fomentou descobertas tão profundas que nos fazem refletir sobre a natureza essencial da realidade, um assunto que tem sido matéria de intenso debate filosófico há milênios. Bibliotecas inteiras poderiam ser montadas contendo somente livros devotados às discussões sobre mecânica quântica, mas nos dedicaremos, por enquanto, apenas a três tópicos, os mais desconcertantes da mecânica quântica: (a) a *dualidade onda/partícula*, (b) o *princípio da incerteza* e, (c) o *emaranhamento quântico*. (STEIN, 2008)

## 3.2 Cinco conceitos para se começar a entender a mecânica quântica

A mecânica quântica é o ramo da Física que estuda os objetos em escala muito pequenas, e a física moderna é dominada pelos seus conceitos.

Durante o século passado, o mundo físico era explicado de acordo com os princípios da mecânica clássica, ou newtoniana. No entanto, no final do século, essa mecânica já não era suficiente para explicar alguns questionamentos que começaram a aparecer. Por isso, foram desenvolvidas as Teorias da Relatividade e da mecânica quântica.

A **Relatividade** (ROVELLI, 2015) é a teoria que descreve a física de objetos muito maciços e de alta velocidade, enquanto a mecânica quântica, ou Física Quântica, estuda a física de objetos muito pequenos.

Muitas das equações da mecânica clássica, que descrevem como as coisas se movem em tamanhos e velocidades no nosso cotidiano, deixam de ser úteis na escala de átomos e elétrons, que agora pode ser explicada pelos princípios da mecânica quântica.

### 3.2.1 As partículas são ondas, e vice-versa

Na escala macroscópica, estamos habituados a dois tipos de fenômenos: ondas e partículas.

As partículas ocupam determinado lugar no espaço, transportando massa e energia à medida que se movem. Já as ondas se propagam por todo o espaço, transportando energia à medida que se movem, mas sem massa.

Quando as partículas colidem, elas assumem trajetórias definidas, que podem ser calculadas por meio das leis de movimento de **Newton**. Já as ondas, quando passam por fendas, geram novas ondas, que ao colidir, podem se reforçar ou se anular.

Porém, na mecânica quântica, essa distinção entre ondas e partículas já não existe. Os objetos que normalmente vemos como partículas, como os elétrons, podem comportar-se como ondas em certas situações, enquanto objetos que normalmente pensamos como ondas, como a luz, podem comportar-se como partículas.

Assim, os elétrons podem criar padrões de difração de onda ao passar por fendas estreitas, assim como as ondas surgem em um lago quando jogamos uma pedra na água. Por outro lado, o efeito fotoelétrico (ou seja, a absorção de luz por elétrons em objetos sólidos) só pode ser explicado se a luz estiver como partícula.

Tais ideias levaram **De Broglie** a concluir que todas as entidades tinham aspectos de onda e de partículas, e que diferentes aspectos eram manifestados de acordo com o tipo de processo submetido. Isso se tornou conhecido como o **Princípio da dualidade Partícula-Onda**.

### 3.2.2 Tudo o que podemos saber são probabilidades

Mas como a **probabilidade** entra no coração da Física ([ROVELLI, 2015](#))? A mecânica quântica prevê que o movimento de cada coisa diminuta ocorre ao acaso. Isso põe em jogo a probabilidade. Podemos não saber alguma coisa de maneira completa, mas podemos atribuir uma probabilidade maior ou menor a alguma coisa. De qualquer modo, para a maior parte dos objetos físicos, nós sabemos algo de seu estado, mas não sabemos tudo, assim, podemos fazer previsões baseadas na probabilidade. Embora não se possa prever tudo exatamente, podemos prever a probabilidade de que aconteça alguma coisa, ou alguma outra coisa. A parte da Física que esclarece essas coisas é a Física Estatística, e um dos trunfos da Física Estatística, a partir de **Boltzmann**, é a de compreender **a origem probabilística do comportamento de certos fenômenos físicos**, como calor, temperatura, ou seja a termodinâmica. A previsibilidade ou imprevisibilidade do comportamento não concernem a um estado exato. Concernem à limitada classe de propriedades do fenômenos, com as quais interagimos. Essa classe de propriedades depende do nosso específico modo de interagir com objetos. Por conseguinte, a probabilidade não concerne a evolução dos corpos e si. Concerne à evolução dos valores de subclasses de propriedades dos corpos quando estes interagem com outros corpos. No decorrer do século XX, a Física Estatística (mecânica estatística), a ciência da probabilidade dos diversos movimentos, foi estendida também aos campos eletromagnéticos e aos fenômenos quânticos ([ROVELLI, 2015](#)).

Quando os físicos usam a mecânica quântica para prever os resultados de uma

experiência, a única coisa que podem prever é a **probabilidade de detectar um dos possíveis resultados**.

Por exemplo, se fizermos um experimento onde um elétron irá parar no lugar A ou B, ao fim, poderemos dizer que existe uma probabilidade de 17% de encontrá-lo no ponto A e uma probabilidade de 83% de encontrá-lo no ponto B. Porém, nunca poderemos dizer com certeza que o elétron definitivamente acabará em A ou em B. Não importa quão cuidadoso seja o preparo de cada elétron, não poderemos saber definitivamente qual será o resultado do experimento. Cada elétron é uma experiência completamente nova, e o resultado final é aleatório.

### 3.2.3 O uso da probabilidade - o *sim*, o *não* e o *talvez*

O uso da probabilidade nos cálculos da Física deu excelente resultado, levando a uma formidável ampliação dos horizontes do conhecimento e a inventos como a TV e o raio laser. Mas a probabilidade também tem as suas limitações e, quando aplicada a uma teoria fundamental, como é o caso da mecânica quântica, provoca certa inquietação. Uma coisa, por exemplo, é alguém olhar um carro em movimento e dizer: "*A velocidade daquele carro é de 100 quilômetros por hora*". Outra, bem diferente, é dizer:

*"Aquele carro não tem velocidade definida; é provável que seja 100 quilômetros por hora, mas também pode ser 80 ou 120"*.

Nas duas situações, existem informações básicas sobre o carro - calcular a velocidade é um dado absolutamente fundamental para qualquer teoria física. Mas, na primeira, a informação é inequívoca: um único número. Em lugar disso, a resposta probabilística fornece um conjunto de números, como se o carro pudesse desenvolver diversas velocidades ao mesmo tempo. Do ponto de vista científico, as respostas múltiplas da mecânica quântica significam apenas isso: a teoria, em certos casos, oferece um conjunto de resultados mais ou menos prováveis para determinado cálculo. Qualquer interpretação, além disso, é simples exercício de imaginação. Um problema é que, no caso de um corpo como o carro, a Física sempre dá uma resposta única e taxativa - **a probabilidade só afeta os corpos microscópicos**.

Esse fato força uma divisão do mundo físico em duas partes, numa das quais valem **leis probabilísticas e deterministas**, e no outro, apenas **leis probabilísticas**. Atualmente, a grande maioria dos cientistas aceita, sem preconceito, as equações probabilísticas. Veja em <https://super.abril.com.br/ciencia/a-revolucao-da-teoria-quantica/>.

### 3.2.4 As correlações quânticas não são locais

Uma das consequências mais estranhas e mais importantes dessa física é a ideia de "emaranhamento quântico". Quando duas partículas quânticas interagem, seus estados irão depender um do outro, independentemente de quão distantes estejam. Você pode segurar uma partícula no Brasil e enviar a outra para Portugal, e depois medi-las simultaneamente. O resultado da medição no Brasil determinará o resultado da medida em Portugal e vice-versa. A correlação entre esses estados não pode ser descrita por qualquer teoria local, na qual as partículas possuem estados definidos. Esses estados são indeterminados até o instante em que um é medido, porém no momento em que os estados de ambos forem determinados, não importa o quão

distante eles estejam. Isso foi confirmado experimentalmente dezenas de vezes ao longo dos últimos trinta anos, com átomos pares, e cada nova experiência reforçou essa teoria. Apesar da medida em Portugal determinar o estado de uma partícula no Brasil, o resultado de cada medida será completamente aleatório. Não há como manipular a partícula portuguesa para produzir um resultado específico no Brasil. A correlação entre as medidas só será evidente após a ação, quando os dois resultados forem comparados, e esse processo deve ocorrer em velocidades mais lentas do que a da luz. O experimento com uma fenda dupla confirma essa indeterminação. Até que a posição do elétron seja medido no lado oposto da fenda, ele poderá existir em todos os caminhos possíveis. Uma partícula quântica pode e vai ocupar vários estados até o momento em que for medida, e após sua medição ela existirá em apenas um estado.

### 3.2.5 A Física quântica é real

Apesar da mecânica quântica ter muitos recursos que desafiam nossa intuição clássica, como os estados indeterminados, medidas probabilísticas e efeitos não locais, ela ainda está sujeita à regras.

Por mais estranhas que sejam suas previsões, a mecânica quântica não contraria os princípios fundamentais da física. Ou seja, você não pode explorar os efeitos quânticos para construir uma nave que viaje na velocidade da luz, ou inventar a telepatia.

A mecânica quântica é uma ciência matemática rigorosa e precisa, e todo efeito que você ouve sobre ela é real e confirmado por experiências.

E onde encontro a física quântica no meu dia-a-dia? A física quântica está ao nosso redor, e determina tudo sobre o mundo em que vivemos. O brilho vermelho no metal quando aquecido e a cor da luz de uma lâmpada de néon são devidos à natureza quântica da luz e dos átomos.

O próprio Sol é alimentado pela física quântica! Se não fosse pelo efeito quântico conhecido como "tunelamento", o Sol não seria capaz de fundir hidrogênio em hélio, produzindo a luz que permite a vida na Terra.

Além disso, os computadores modernos que temos são construídos em chips de silício, que contém milhões de pequenos transistores. Sem entender a física quântica de como átomos e elétrons agem, seria impossível construir um único transistor, e muito menos milhões deles.

As redes de telecomunicações modernas, como a Internet, também dependem da mecânica quântica. Nelas, as informações são transmitidas por meio de pulsos de luz que viajam por cabos de fibra óptica.

Esses pulsos de luz são produzidos por lasers de diodo, que usam pequenos chips de semicondutores para gerar feixes intensos de luz. A construção dos lasers que carregam a Internet seria impossível sem entender a física quântica dos semicondutores e a natureza quântica da luz.

Ou seja, muito da tecnologia que temos hoje em dia existe graças à mecânica quântica.



### 3.3 A revolução da Teoria Quântica

*A teoria quântica não mudou apenas as ideias dos cientistas sobre o comportamento da matéria. Mudou a própria ideia de matéria. Dentro do átomo, nada estaria definido, tudo seria probabilidade. (Paul Davis)*<sup>1</sup>

As verdadeiras revoluções científicas são aquelas que além de ampliar os conhecimentos existentes, se fazem também acompanhar de uma mudança nas ideias básicas sobre a realidade. Um exemplo célebre foi a revolução do polonês **Nicolau Copérnico** no século XVI, que derrubou o conceito segundo o qual a Terra estava imóvel no centro do Universo, afirmando em vez disso que nosso planeta gira em torno do Sol. Depois, o inglês **Isaac Newton** suplantou o conceito de *espaço absoluto* e dois séculos mais tarde o alemão **Albert Einstein** aposentou também a ideia do *tempo absoluto*. Embora importantes, nenhuma dessas grandes revoluções na ciência pode rivalizar com o impacto da revolução quântica. A partir dela, os físicos foram forçados a abandonar, não apenas os conceitos do homem sobre a realidade - mas a própria realidade. Não admira que a Física Quântica tenha adquirido a reputação de algo bizarro ou místico. Tanto que o dinamarquês **Niels Bohr**, um dos criadores da nova ciência, chegou a afirmar certa vez que só não se escandalizou com a Física Quântica quem não a entendeu.

O ponto de partida para chegar às ideias quânticas é o átomo, já conhecido dos filósofos gregos, na Antiguidade. Eles acreditavam que toda matéria era constituída por minúsculos fragmentos indestrutíveis. Ora, o domínio da Física Quântica é formado justamente pelos fragmentos desses fragmentos. Desde 1909, de fato, o inglês **Ernest Rutherford** estabeleceu que os átomos, aparentemente indivisíveis, são compostos por um núcleo ao redor do qual giram outras partículas, os elétrons. Segundo esse modelo, o núcleo podia ser comparado ao Sol, enquanto os elétrons seriam os planetas orbitando a sua volta. É importante salientar a ideia de que os elétrons seguiam trajetórias bem definidas, de tal modo que a qualquer momento seria possível determinar a sua posição e a sua velocidade.

O problema é que, ao contrário dos planetas, os elétrons não seguem um trajeto claro e inequívoco quando se movem. Seus caminhos caprichosos só seriam revelados anos depois do modelo atômico proposto por **Rutherford**. O primeiro sinal de que a visão "planetária" não funcionava surgiu em 1911, quando **Neils Bohr** escreveu uma nova fórmula sobre a emissão de energia pelos átomos. Para surpresa geral, a fórmula mostrava que havia lugares proibidos para o átomo - regiões inteiras, em torno do núcleo atômico, onde os elétrons não podiam girar. Podiam saltar de uma órbita mais distante a outra mais próxima, mas não podiam ocupar diversas órbitas intermediárias. E, nesse caso, emitiam um pacote inteiro de energia - nunca menos de certa quantidade bem definida, desde então chamada *quantum* de energia.

Era estranho, já que os planetas podiam girar a qualquer distância do Sol e mudar de órbita alterando o seu nível energético em qualquer quantidade, sem limite. Apesar disso, a fórmula de **Bohr** explicava com precisão os fatos conhecidos sobre a emissão de luz pelos átomos, de modo que a nova Física do *quantum* acabou se impondo com

---

<sup>1</sup> Paul Davis - É um desenvolvedor de software britânico mais conhecido por seu trabalho em software de áudio (JACK) para o sistema operacional Linux e por seu papel como um dos primeiros programadores da Amazon.com.

firmeza. Dez anos mais tarde, o enigma das órbitas proibidas foi resolvido de uma maneira que afastou ainda mais do átomo a ideia de um sistema solar em miniatura. Desde a década de 20, com efeito, as órbitas dos elétrons passaram a ser vistas como algo semelhante às ondas sonoras que compõem as notas de um instrumento musical: portanto, uma imagem muito distante dos corpos sólidos girando em torno do Sol.

O primeiro passo na direção das ondas eletrônicas surgiu em experiências nas quais um feixe de elétrons atravessava um cristal e se espalhava mais ou menos como a luz ao formar um arco-íris. O físico francês **Louis de Broglie** mostrou que o comprimento dessas inesperadas ondas podia ser relacionado com a velocidade dos elétrons. Segundo **De Broglie**, elétrons em alta velocidade se comportam como ondas curtas e elétrons em baixa velocidade, como ondas longas. Assim, tornou-se possível transformar uma característica dos movimentos mecânicos - a velocidade - em um traço típico dos fenômenos ondulatórios, o comprimento de onda.

Essa foi a deixa que o alemão **Erwin Schrodinger** aproveitou para criar a imagem musical do átomo mostrando que ela desvelava o enigma das órbitas proibidas. Basta ver que, ao vibrar, uma corda de violão produz uma nota fundamental, como o mi por exemplo, e diversas outras notas geralmente inaudíveis, que enriquecem o som mais forte. São os chamados harmônicos, cujas vibrações são sempre múltiplos inteiros da vibração principal: pelo menos duas vezes mais rápidas do que esta, mas nunca 2.5 vezes, ou 3.5 vezes. O mesmo ocorre no átomo, imaginou **Schrodinger**: nesse caso, o elétron só gira onde o tamanho da órbita lhe permite formar ondas inteiras, excluindo as órbitas que, para serem completadas, exigiriam uma fração de onda.

O resultado confirmava a fórmula intuitiva de **Bohr**, dando início a uma nova teoria física, daí para a frente chamada mecânica quântica. Sua grande marca foi a introdução do conceito de *onda* de maneira tão fundamental quanto a noção de *partícula*. Coube ao alemão **Max Born**, outro dos grandes pioneiros do século, explicar **como um elétron podia ser ao mesmo tempo onda e partícula**. Para ele, a *onda* não era nenhum tipo de substância material, mas um meio de avaliar certas medidas, como a velocidade ou a posição de uma partícula, "Onda eletrônica", na verdade, seria uma expressão com o mesmo sentido que se atribui à expressão "onda de criminalidade". Assim, quando há uma onda de crimes numa cidade, há grande probabilidade de um crime ocorrer nessa cidade, a qualquer momento.

A *onda* associada a um elétron descreve a distribuição estatística dessa partícula, determinando onde é mais provável que ela esteja. A ondulação nada tem a ver com a substância do elétron, mas em cada ponto do espaço diz qual a probabilidade de que ele se encontre ali. Essa interpretação de **Max Born** poderia parecer frustrante para quem esperasse ver as ondas ligadas a algum segredo sobre a natureza da matéria, mas é uma mudança na própria ciência. Até então, havia grande convicção de que o Universo fosse estritamente determinístico e de que, portanto, sempre se poderia conhecer com precisão a posição de um corpo. Para a mecânica quântica, porém, o Universo é inerentemente não-determinístico, uma ideia que **Albert Einstein** nunca aceitou. "Deus não joga dados com o Universo", respondia ele aos que argumentavam em favor da *probabilidade quântica*. Mas existe um método poderoso para tentar adivinhar os lances dos dados divinos: trata-se do célebre **Princípio da Incerteza**, enunciado pelo físico **Werner Heisenberg** em 1927.

Sua base é uma fórmula para medir pares de valores, como por exemplo veloci-

dade e posição. O princípio diz que, se a posição for medida com grande precisão, é possível ter uma certa ideia do valor da velocidade. Se, em vez disso, se medir a velocidade com precisão, a posição pode ser avaliada dentro de certos limites. A regra vale para outros pares de valores, como tempo e energia. Muitas vezes, o princípio tem sido explicado como uma interferência do medidor sobre o objeto medido: para saber a posição de um elétron é preciso agir sobre ele, por meio de um raio de luz, por exemplo. O raio incide sobre o alvo e, dependendo do desvio que sofre permite avaliar a posição do alvo.

É o mesmo procedimento que se usa para ver um objeto grande, como um carro, e determinar onde está. É claro que o levíssimo impacto de um ponto de luz não tem nenhum efeito mensurável sobre o movimento do carro, enquanto no caso do elétron o choque é devastador, perturbando a medição. Em consequência, haveria uma incerteza inerente a toda medição em escala microscópica. Na realidade, segundo a concepção moderna, não há sentido dizer que um elétron tem ao mesmo tempo posição e velocidade bem definidas. A incerteza seria inseparável da própria natureza dos corpos quânticos.

É mais fácil imaginar que um elétron tem duas caras - como um ator desempenhando dois papéis em um filme. Ao medir sua posição, se estará observando O "*elétron-em-posição*", um dos papéis do ator. O "*elétron-em-velocidade*" entra em cena quando se faz uma medida de velocidade. No primeiro caso, o elétron se assemelha mais a uma partícula, já que a imagem que temos é a de um corpo bem localizado no espaço. Quando a medida mais precisa é a da velocidade e o corpo não tem uma posição definida - há diversos lugares com igual *probabilidade* - então surge com mais força a sua característica de onda.

A experiência que melhor ressalta a dupla face dos elétrons é a das fendas de interferência, inicialmente realizada com luz pelo inglês **Thomas Young**, no início do século XIX. A comparação com a luz é importante. Um raio luminoso é dirigido para uma tela com uma estreita fenda de modo a projetar uma imagem difusa em uma segunda tela colocada atrás da primeira. Se a primeira tela tiver duas fendas em vez de uma, surgirão duas imagens difusas, mais ou menos circulares, que se sobreporão parcialmente. Mas as imagens sobrepostas não se tornam uma simples soma de luzes: em vez disso, aparecem diversas faixas intercaladas de luz e sombra. São as chamadas franjas de interferência.

O mesmo efeito é obtido se, em lugar de luz, se usar um feixe de elétrons. A franja eletrônica, desenhada em uma tela de TV, é uma demonstração da natureza ondulatória do elétron. As faixas "claras", nesse caso, representam as posições onde é mais provável encontrar os elétrons. É impossível explicar a interferência de elétrons por meio da noção tradicional de partícula mecânica. É claro que um elétron não pode passar pelas duas fendas ao mesmo tempo, pelo menos enquanto se mantiver apenas como uma partícula, à maneira antiga. Mas a interferência é uma combinação daquilo que acontece nas duas fendas ao mesmo tempo. Então, se o elétron passa por uma única fenda, como será que a existência da outra fenda, por si só, pode criar as franjas claras e escuras?

A resposta é que a partícula está se comportando como uma onda. Mesmo quando só um elétron é atirado contra as fendas, o padrão de interferência surge na tela, interferindo, por assim dizer, consigo mesmo. Segundo o princípio da incerteza é

possível fazer uma medida precisa da posição do elétron e decidir em qual das duas fendas ele está, mas o preço a pagar é uma perda de precisão sobre o rumo que ele tomará em seguida. De modo que se terá apenas uma vaga ideia de seu movimento entre uma placa e outra: a maior probabilidade é de que na segunda placa se formará uma imagem difusa e aproximadamente circular.

Não é possível avaliar a precisa distribuição de claros e escuros das franjas de interferência. Caso se queira medir diretamente esse padrão, será preciso abandonar qualquer pretensão de saber por qual fenda o elétron passou: é igualmente provável que tenha passado por qualquer uma delas, o que significa uma incerteza sobre sua posição. Um meio de entender tudo isso é imaginar que existam dois mundos, de tal forma que em um deles o elétron passe pela primeira fenda e no outro, pela segunda. Os dois mundos coexistem, misturando suas realidades, até o momento em que se faça uma medida direta da posição do elétron. Nesse caso, as franjas de interferência - formarão uma realidade bem definida apenas enquanto não se medir a posição do elétron em uma ou outra fenda.

O fato é que os pesquisadores podem escolher o que querem ver - uma outra face do elétron - e por isso se costuma dizer que a natureza do elétron depende do homem. Nem todos os físicos levam a sério a ideia de duas realidades existindo uma ao lado da outra, mas é possível puxar pela imaginação e penetrar ainda mais profundamente nos seus paradoxos. No caso do experimento com as franjas de interferência, o que aconteceria se o feixe de elétrons dirigido para as fendas alcançasse a segunda tela, sem que ninguém observasse o resultado? A tela poderia ser fotografada e a foto, arquivada, para que não fosse vista. Assim, algo teria acontecido, mas, como não foi observado, não poderia existir como realidade concreta - até que alguém finalmente se decidisse a lançar um olhar criador para o fantasma perpetuado no filme.

Trata-se de um célebre quebra-cabeça criado por **Erwin Schrodinger** e desde então apelidado "paradoxo do gato". Esse experimento mental, como dizia o físico, funciona da seguinte forma: um gato é aprisionado numa caixa junto com uma garrafa selada contendo gás venenoso. Sobre a garrafa pende um martelo pronto para quebrá-la. O gatilho dessa armadilha é uma substância radioativa que emite partículas a alta velocidade. Em 1 minuto, há uma chance de 50% de que a substância emita radiação e solte o martelo, fazendo quebrar a garrafa e liberar o gás venenoso. Assim, ao cabo de 1 minuto, coexistem dois mundos possíveis. Num deles, o gatilho foi acionado e o gato está morto; no outro, não houve emissão de radiação e o gato está vivo. Enquanto não se abrir a caixa, nenhuma das duas possibilidades poderá ser considerada real e o gato não será muito diferente dos mortos-vivos das histórias de terror. Ele permanece numa superposição de realidades, entre a vida e a morte.

O físico inglês **Anthony Leggett** imagina que os enigmas quânticos não valem para os gatos - eles são complexos demais, do ponto de vista físico, para ficarem suspensos entre dois mundos-fantasmas. A mecânica probabilística está definitivamente confinada ao universo das partículas fundamentais, as formas mais simples da

O físico americano **Eugene Wigner**, por sua vez, criou uma especulação radical segundo a qual é a mente do físico que cria toda a realidade. Seria a consciência do homem que filtra a confusão quântica do Universo e gera uma realidade bem definida. **Roger Penrose** é outro cientista a imaginar um entrelaçamento entre a mente e a realidade. Ele pensa que os mecanismos mentais do raciocínio estão submetidos às flutuações quânticas, dando origem, por exemplo, às inexplicáveis

explosões criativas dos músicos ou dos matemáticos. Muitos pensadores, como **Fritjof Capra**, supõem além disso um paralelo entre a realidade quântica e as concepções místicas orientais.

Todas essas especulações indicam como são profundos os paradoxos que, há sessenta anos, entraram para os livros de Física por meio da mecânica quântica. O fato de continuarem sendo debatidos por tanto tempo pode não impressionar aqueles cientistas para os quais as teorias servem apenas como instrumento de trabalho. Mas poucos adotariam a opinião radicalmente cética de **Einstein** que, nas suas próprias palavras, enterrou a cabeça na areia "de medo do temível quantum".

### 3.4 Bibliografia e Fonte de Consulta

Os 5 conceitos para entender mecânica quântica - <<https://www.hipercultura.com/entendas-os-principais-conceitos-da-mecanica-quantica/>>

A revolução quântica - <https://super.abril.com.br/ciencia/a-revolucao-da-teoria-quantica/>

À procura do gato de Shrodinger, John Gribbin, Editorial Presença, Lisboa, 1986

Pensando a Física, Mário Schenberg, Editora Brasiliense, São Paulo, 1984.

### 3.5 Referências e Leitura Recomendada

Schrödinger, E. (1926). *An Undulatory Theory of the Mechanics of Atoms and Molecules (PDF)*. *Physical Review (em inglês)*. 28 (6): 1049-1070. Bibcode:1926PhRv...28.1049S. doi:10.1103/PhysRev.28.1049

Griffiths, David J. (2004). *Introduction to Quantum Mechanics* (2nd ed.) (em inglês). Upper Saddle River, Nova Jérsei: Prentice Hall. ISBN 0-13-111892-7

Ballentine, Leslie (1998). *Quantum Mechanics: A Modern Development* (em inglês). Nova Jérsei: World Scientific Publishing Co. ISBN 9810241054

Laloe, Franck (2012). *Do We Really Understand Quantum Mechanics* (em inglês). Cambridge: Cambridge University Press. ISBN 978-1-107-02501-1

Fleming, Henrique. *A energia e a equação de Schrödinger*. e-física.

Martins, Jorge Sá. *Equação de Schrödinger*. Youtube. 21 de jun de 2011.

Martins, Jorge Sá. *A Equação de Schrödinger em 2 e 3 Dimensões*. Youtube. 6 de set de 2011.

Martins, Jorge Sá. *Oscilador Harmônico Quântico*. Youtube. 19 de jul de 2011.

Karl Grandin, ed. (1933). Erwin Schrödinger Biography <[http://nobelprize.org/nobel\\_prizes/physics/laureates/1933/schrodinger-bio.html](http://nobelprize.org/nobel_prizes/physics/laureates/1933/schrodinger-bio.html)>. Les Prix Nobel (em inglês). The Nobel Foundation. Consultado em 29 de julho de 2008.

# A Base Experimental da Mecânica Quântica

A Física de partículas (partícula é uma concentração localizada de massa cujas dimensões mostrem-se desprezíveis em relação às demais dimensões espaciais), estudada pela mecânica quântica (parte da Física Moderna), busca o fundamental, o nível mais básico da matéria e da Natureza. Todo o nosso mundo visível se fundamenta nesse nível invisível das partículas elementares. Podemos chamar de *partículas elementares* toda a porção indivisível da matéria (aparentemente não tem tamanho, mas podem ter massa) como os *léptons* (elétron  $e$ , pósitron  $e^+$ , múon  $\mu$ , tauon  $\tau$ , neutrinos, antineutrinos) e os *hádrons* (tem tamanho e uma estrutura interna) como os (prótons, neutrons, quarks). O físico americano **Murray Gell-Mann** (1929-) propôs um modelo onde os *hádrons* eram constituídos de partículas que ele chamou de *quarks*. Os hádrons, prótons (compostos de *quarks*) e neutrons (compostos de *quarks*), são constituídos de combinações de *quarks* chamadas de *bárions* ou *mésons* (PIRES; CARVALHO, 2014).

Em física de partículas e na química quântica, *antimatéria* é a extensão do conceito de antipartícula da matéria, por meio de que a *antimatéria* é composta de antipartículas da mesma maneira que a matéria normal está composta das partículas subatômicas (JUNIOR, 2018). Como *antipartículas* das partículas subatômicas, temos, por exemplo, as antipartículas *pósitrons* (elétrons com carga positiva), *antiprótons* (prótons com carga negativa) e *antinêutrons* (com carga nula como os nêutrons) poderiam dar forma a *antiátomos* da mesma maneira que elétrons, prótons e nêutrons dão forma a *átomos* normais da matéria. Quando o pósitron é "aniquilado" com um elétron, as massas de ambos são totalmente transformadas em *fótons* (radiação gama)  $\gamma$ . O sistema formado por um pósitron e um elétron, formando um *átomo exótico*, é definido como um átomo normal em que uma ou mais partículas sub-atômicas foram "substituídas" por outras partículas de mesma carga. Um fóton surge quando ocorre a transição de um elétron de um átomo entre dois estados de energias diferentes, o elétron ao passar de uma camada mais interna para uma mais externa, ao receber energia e retornar para o estado inicial, emite a energia correspondente a essa diferença. Também, uma partícula tem a tendência de "*decair ou se transformar*" em outras partículas, a não ser que uma lei de conservação impeça esse decaimento.

A *física de partículas* é um ramo da Física que estuda os constituintes elementares da

matéria e da radiação, e a interação entre eles e suas aplicações. É também chamada de Física de altas energias, porque muitas partículas elementares só podem ser criadas a energias elevadas, logo a detecção destas também é possível apenas a altas energias de aceleração. O *elétron* e o *próton* foram as únicas partículas aceleradas até os dias de hoje. Outras nunca foram nem detectadas e as restantes foram detectadas através da radiação cósmica. O *elétron* é uma partícula subatômica, com carga elétrica negativa. O *próton* é uma partícula subatômica, com uma carga elétrica positiva. O *neutron* é uma partícula subatômica, eletricamente neutro. Os *prótons* e os *neutrons* são referidos coletivamente como "núcleon". *Prótons* e *neutrons* estão presentes no núcleo de um átomo. O núcleo atômico é constituído por *prótons*, que possuem carga elétrica positiva, e *neutrons* que possuem ambas as cargas elétricas (negativa e positiva), o que o torna neutro. Um átomo é uma unidade básica de matéria que consiste num núcleo central de carga elétrica positiva envolto por uma nuvem de elétrons de carga negativa. Os *elétrons* de um átomo estão ligados ao núcleo por força eletromagnética. Da mesma forma, um grupo de átomos pode estar ligado entre si através de ligações químicas baseadas na mesma força eletromagnética, formando uma *molécula*.

A mecânica quântica é a teoria que descreve corretamente a estrutura e as propriedades dos átomos. O conjunto dos *prótons* e *neutrons*, ligados entre si num átomo, formam o núcleo atômico. Em 1913, o físico **Niels Bohr** propôs um modelo no qual se assumia que os *elétrons* de um átomo orbitavam o núcleo, mas que só o podiam fazer ao longo de um conjunto finito de órbitas e que podiam saltar entre essas órbitas, apenas através de alterações de energia correspondentes à absorção ou radiação de um *fóton*. (PIRES; CARVALHO, 2014)

O *fóton* é a partícula elementar mediadora da força eletromagnética. O *fóton* também é o *quantum da radiação eletromagnética* (incluindo a luz). O termo *fóton* foi criado por **Gilbert Newton Lewis** em 1926 (LEWIS, 1926). *Fótons* possuem *spin*. A troca de fótons entre as partículas como os elétrons e os prótons é descrita pela eletrodinâmica quântica, a qual é a parte mais antiga do modelo padrão da física de partículas. Ele interage com os elétrons e núcleo atômico sendo responsável por muitas das propriedades da matéria, tais como a existência e estabilidades dos átomos, moléculas, e sólidos. Em alguns aspectos, um *fóton* atua como uma partícula, sendo que a explicação satisfatória para esse efeito foi dada em 1905, por **Albert Einstein** pelo *Efeito fotoelétrico*. Em outras ocasiões, um *fóton* se comporta como uma *onda*, quando passa através de uma lente ótica. De acordo com a conhecida *dualidade partícula-onda* da mecânica quântica, é natural para um *fóton* apresentar ambos aspectos na sua natureza, de acordo com as circunstâncias em que se encontra. Normalmente, a luz é formada por um grande número de fótons, tendo a sua intensidade ou brilho ligada ao número deles (AMSLER, 2008). O fóton não tem uma massa de repouso, ele não pode estar em repouso, pois surge com velocidade, lembramos que no instante que ele nasce é lhe constituído como tendo a velocidade da luz.

Um *estado quântico* é qualquer estado possível em que um sistema mecânico quântico possa se encontrar. Um estado quântico plenamente especificado pode ser descrito por um **vetor de estado** (num espaço de **Hilbert 8**), por uma **função de onda** ou por um *conjunto completo de números quânticos* para um dado sistema. Ao *estado quântico de menor energia* possível dá-se o nome de *estado quântico fundamental*.

O fato de ser impossível atribuir ao mesmo tempo uma posição e uma velocidade exatas a uma partícula, renunciando-se assim ao conceito de trajetória, é vital em Mecânica clássica. Ao invés da trajetória, o movimento de partículas em mecânica

quântica é descrito por meio de uma **função de onda**, que é uma função da posição da partícula e do tempo. A *função de onda* é interpretada por **Max Born** como uma medida da probabilidade de se encontrar a partícula em determinada posição e em determinado tempo. Esta interpretação é a mais aceita pelos físicos hoje, no conjunto de atribuições da mecânica quântica regulamentados pela escola de Copenhagen. Para descrever a dinâmica de um sistema quântico deve-se, portanto, achar sua *função de onda*, e para este efeito usam-se as equações de movimento, propostas por **Werner Heisenberg** e **Erwin Schrödinger**, independentemente.

Na mecânica quântica o termo *spin* (em inglês "giro") associa-se, sem rigor, às possíveis orientações que partículas subatômicas carregadas, como o próton e o elétron, e alguns núcleos atômicos podem apresentar quando imersas em um campo magnético. o termo *spin* é encarado simplesmente como um quarto número quântico. Os números quânticos descrevem as energias dos elétrons nos átomos e são de enorme relevância quando se trata de descrever a posição dos elétrons nos átomos. Números quânticos são necessários à definição dos *estados quânticos* destas partículas quando em estados discretos de energia em sistemas confinados, a exemplo nos orbitais em um átomo. O termo *spin* em mecânica quântica liga-se ao vetor *momento angular* intrínseco de uma partícula e às diferentes orientações (quânticas) deste no espaço.

*Momento angular* (quantidade de movimento angular) de um corpo é uma grandeza física associada à rotação desse corpo. Deve-se dizer que, com o advento da mecânica quântica, o status da grandeza física quantidade de movimento angular sofreu uma severa modificação. A grandeza não pode, no contexto da mecânica quântica, ser definida em termos de duas grandezas que são relacionadas pelo *princípio da incerteza* como o *raio vetor* e a *velocidade angular*. Tais grandezas são complementares e não podem ser, simultânea e de forma totalmente precisa, determinadas. A pares de grandezas assim relacionadas dá-se o nome de grandezas complementares.

*Raios cósmicos* são partículas extremamente penetrantes, dotadas de alta energia, que se deslocam a velocidades próximas a da luz no espaço sideral. Portanto, raios cósmicos não são raios, mas partículas.

## 4.1 A luz é onda ou partícula?

É provável que nenhuma outra questão na ciência tenha causado maior controvérsia por um período de tempo do que a natureza da luz. Filósofos gregos e medievais especulavam sobre essa questão, dispondo teorias que diziam que a luz era uma substância, ou que era uma onda, ou uma vibração. Quase dois milênios se passaram, quando Isaac Newton apareceu e entrou no debate. Newton, além da Matemática, Mecânica ou Gravitação, inventou a ciência da Óptica. **Newton**, acabou por definir a natureza da luz como uma *substância*. (STEIN, 2008)

Uma substância, em Química, é qualquer espécie de matéria formada por átomos de elementos específicos em proporções específicas. Cada substância possui um conjunto definido de propriedades e uma composição química. Elas também podem ser inorgânicas (como a água e os sais minerais) ou orgânicas (como a proteína, carboidratos, lipídeos, ácido nucleico e vitaminas). Todas as substâncias químicas possuem a unidade de sua estrutura (moléculas) iguais entre si; possuem composição e características fixas, não há alteração da temperatura durante os processos de



mudanças de Estados físicos da matéria (como fusão e ebulição); sua composição fixa garante que podem ser representados com fórmulas. Conhecemos as características das substâncias, mas quais são as características das ondas? Nem todas as ondas se comportam da mesma maneira. O som, um exemplo clássico de uma onda, pode fazer curvas, Mas, a luz não pode. Ondas de água podem interferir entre si. Por mais de um século, poucos esforços foram feitos quer para afirmar ou negar a teoria da luz como onda. Mesmo que **Christian Huygens** (1629-1695) favorecesse a ideia de que a luz era um fenômeno ondular.

Quem, enfim, realizou o experimento definitivo foi **Thomas Young** (1773-1829). Ele fez contribuições significativas para a teoria dos materiais, descrevendo a elasticidade de substâncias. Ele construiu uma teoria sobre a visão das cores, observando que, para ser capaz de enxergar todas as cores, era somente necessário ser capaz de enxergar o vermelho, o azul e o verde.



*Thomas Young*

Figura 41 – Thomas Young - Conhecido pela experiência da dupla fenda, que em 1802 possibilitou a determinação do carácter ondulatório da luz.

Fonte: <[https://pt.wikipedia.org/wiki/Thomas\\_Young](https://pt.wikipedia.org/wiki/Thomas_Young)>

O fascínio de **Young** pelos olhos levou-o a iniciar investigações sobre a visão das cores e sobre a *natureza da luz*. Em 1802, ele executou o experimento que mostraria, de uma vez por todas que **a luz era um fenômeno ondulatório**: a **experiência da dupla fenda**, que possibilitou a determinação da natureza ondulatória da luz.

## 4.2 Einstein e o efeito fotoelétrico

O experimento da dupla fenda de **Young** parecia encerrar a questão relativa ao fato de a luz ser uma onda ou uma partícula - até que **Albert Einstein** (1879-1955) deu sua contribuição, em 1905. Um dos seus artigos da época explicava o *efeito fotoelétrico*. Quando a luz recai sobre um material fotoelétrico, como por exemplo, o selênio, a energia na luz é algumas vezes suficiente para jogar elétrons para fora da superfície do metal. A luz pode produzir eletricidade, daí o nome *fotoelétrico*.

A teoria das ondas de luz previa que, quanto maior era a intensidade da luz, maior seria a energia dos elétrons emitidos. Num experimento clássico feito em 1902, **Philipp Lenard** (1862-1947) mostrou que não era o caso, e que a energia dos elétrons emitidos era independente da intensidade da luz. Não importava quão forte fosse a fonte de luz, os elétrons emitidos tinham a mesma energia. **Lenard** também mostrou que a energia dos elétrons emitidos dependia da cor da luz incidente; se fosse usada uma luz de *menor comprimento de onda*, a energia dos elétrons emitidos era maior do que se fosse usada uma luz de *comprimento de onda maior*.



Figura 42 – Philipp Lenard - A energia dos elétrons emitidos era independente da intensidade da luz.

Fonte: <[https://pt.wikipedia.org/wiki/Philipp\\_Lenard](https://pt.wikipedia.org/wiki/Philipp_Lenard)>

O orientador de **Lenard** na University of Heidelberg, o químico alemão, **Robert Bunsen** (1811-1899) havia descoberto que os padrões de luz, reconhecidos com faixas de cores diferentes, caracterizavam cada elemento. Esse experimento seminal fez com que **Lenard** merecesse o Prêmio Nobel em 1905, o mesmo ano em que **Einstein** explicava as razões por trás dos fenômenos que **Lenard** viria a descobrir.



Figura 43 – Robert Bunsen - Os padrões de luz, reconhecidos com faixas de cores diferentes

Fonte: <<https://pt.wikipedia.org/wiki/RobertBunsen>>

**Einstein** explicou o efeito fotoelétrico através da ideia de **Planck** sobre os *quanta*. Ele presumiu que a luz se comportava como uma coleção de partículas, onde cada partícula é chamada um *fóton*. E cada fóton carregando uma energia que dependia da frequência da luz. Quanto menor o comprimento de onda, maior a energia do *fóton*. Quando os fótons de alta energia (com menor comprimento de onda) atingem um elétron com energia suficiente para jogá-lo para fora do metal, aquele elétron adquire mais energia, do que quando atingido por um fóton de maior comprimento de onda (baixa energia). A explicação do efeito fotoelétrico deu a **Einstein**, o Prêmio Nobel em 1921. (STEIN, 2008)

### 4.3 A matéria é onda ou partícula? -1924

Em 1924, **Louis Broglie** (1892-1987) escreveu uma tese, na qual lançava a nova ideia de que a matéria também poderia ter qualidades similares às das ondas. A tese concluía uma única equação expressando uma relação simples entre o *comprimento de onda da partícula* (obviamente, uma propriedade de onda) e seu *momento* (uma propriedade da partícula, definida em termos de sua massa e sua velocidade). Em 1927, isso foi experimentalmente confirmado, e **Broglie** recebeu o Prêmio Nobel de 1929.

Para entender essa notável ideia, imagine que ajustemos o *spray* de tinta que descrevemos anteriormente de modo que as partículas de tinta saiam em linha reta, e bem lentamente. - talvez uma única partícula de tinta a cada poucos segundos. Direcionamos esse *spray* de tinta para a formação de duplas fendas e, após esperarmos um período de tempo, olhamos por trás das fendas para ver como está a peça de papelão traseira. Sem surpresa alguma, sua aparência é basicamente igual a quando usamos o *spray* com o jato máximo - as duas manchas de margens difusas centradas



Figura 44 – Louis Broglie - A natureza ondulatória dos elétrons.

Fonte: <[https://pt.wikipedia.org/wiki/Louis\\_de\\_Broglie](https://pt.wikipedia.org/wiki/Louis_de_Broglie)>

atrás de cada uma das duas fendas.

Partículas microscópicas, como elétrons, têm um comportamento peculiar ao passar por uma fenda dupla. Este comportamento é diferente tanto de projéteis como de ondas. Ele tem características de ambos, o que designamos como *dualidade onda-partícula*. É necessário aprender também a usar a matemática das ondas para calcular as probabilidades de encontrar o elétron em determinadas posições do espaço. (<<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula02.pdf>>)

Execute esse mesmo experimento usando , em vez de spray de tinta, um *canhão de elétrons*, disparando elétrons em vez de partículas de tinta (e usando um detector que registra o impacto de cada elétron, iluminando cada pixel no ponto de impacto), e algo estranho e totalmente inesperado acontecerá. Em vez de duas manchas de luz com margens difusas, veremos franjas escuras e franjas claras em alternância - a assinatura da interferência de onda. A conclusão é - sob tais circunstâncias, o elétron se comporta como uma onda. **A matéria, como a luz, algumas vezes se comporta como partícula; outras vezes, como onda.** (STEIN, 2008)

## 4.4 Decisões divididas: Experimentos com divisores de feixes

Para o entendimento desta seção lançaremos mão do campo de jogo de Baseball, em alusão ao experimento com **divisores de feixes**.

#### 4.4.1 O Campo

O campo de Baseball tem um território válido e um território inválido. Duas linhas laterais ("foul lines") que seguem perpendicularmente do "home plate" aos fundos, demarcam o território válido dentro que as jogadas acontecem (com algumas exceções). O território válido tem duas partes: o campo interno ("infield") e o campo externo ("outfield").

Campo Interno ("Infield") - Os pontos principais do campo interno são: a Primeira (1ª) Base, a Segunda (2ª) Base, a Terceira (3ª) Base, o "Home Plate" (casa-base) e a Placa de Arremessador.

Campo Externo ("Outfield") - O campo externo, também chamado os fundos, é grande e é dividido em três áreas gerais (não marcadas): o Fundo Direto, o Fundo Central e o Fundo Esquerdo.

Dimensões de um campo de beisebol - Um campo de baseball ocupa um área equivalente a quase dois campos de futebol. Não há medidas oficiais para o tamanho de campo, mas tipicamente a distância do "home plate" ao limite do campo é aproximadamente (100 m) ao longo das linhas laterais aumentando a mais que (120 m) no centro. O campo interno tem medidas oficiais: (27,4 m) entre as bases que formam um diamante com a placa de arremessador localizada a (18,4 m) do "home plate". É comum se chamar as partes do campo pelos nomes abreviados: primeira, segunda, terceira, "home", esquerdo, centro, e direito. Um campo de baseball é representado na Figura 46 seguinte.



Figura 45 – Componentes de um campo de Baseball.

Fonte: Google Images

#### 4.4.2 O que é Baseball - uma breve explicação

O *basebaal* é um jogo composto por dois times de nove jogadores que se alternam entre turnos de ataque e defesa. Uma partida é dividida em "entradas" que consistem

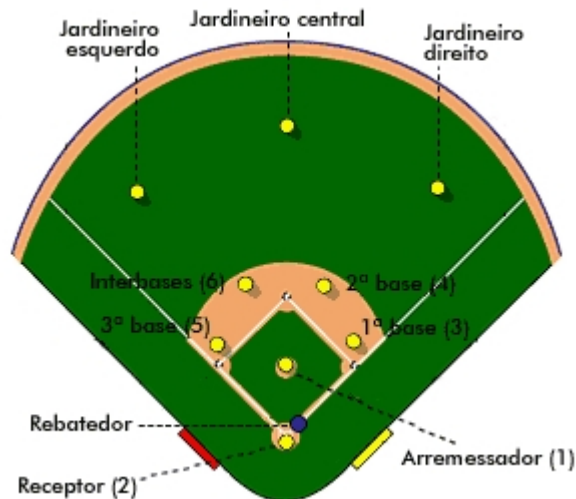


Figura 46 – Um campo de Baseball - a posição dos jogadores.

Fonte: <<https://ceramicabeisebol.com/beisebol/>>

em dois turnos: um time ataca no primeiro turno e defende no segundo, e vice-versa. No ataque, os jogadores, um por vez, entram em campo no "home plate" com um bastão, a fim de rebater a bola lançada pelo arremessador do time adversário que está na defesa. Se um rebatedor acerta a bola na área válida, ele torna-se corredor e tenta alcançar em seguida, a primeira, segunda e terceira base sem ser eliminado pela defesa, até que chega novamente ao "home plate". Ele não precisa completar a volta em uma jogada só, podendo avançar uma ou mais bases por vez durante os rebatimentos dos seus colegas. Cada volta completada marca um ponto, chamado de "corrida", para o time no ataque. Um time continua no ataque até que três jogadores sejam eliminados, aí então acontece uma troca, e o time que atacava vai para a defesa e, o que defendia vai para o ataque. Ao final da partida, o time que marcou mais corridas vence. Em caso de empate, são disputadas entradas extras até que se tenha um vencedor.

As Tarefas Básicas do Baseball - Objetivos:

Defesa - (c) **Lançar, Apanhar/Pegar**. Tem que **eliminar atacantes** sem ceder pontos.

Ataque - (a) **Rebater** (b) **Correr as bases**. Atacantes tem de **marcar pontos através de rebatidas** e **fazer os percursos das bases** sem ser eliminado.

#### 4.4.3 O experimento com divisores de feixes

Uma série de experimentos intrigantes nessa área são conduzidos com *divisores de feixes*. Pode-se suspeitar que os fótons simplesmente assumem um ou outro comportamento - **onda** ou **partícula** - quando atingem o divisor de feixes.

Imaginemos que um fóton (um atacante-rebatedor) comece sua jornada numa das bases de um campo de baseball e consiga um duplo, conseguindo dar dois saltos no percurso das bases, passando para a segunda base. Nesse experimento o fóton pode chegar à segunda base passando pela rota usual - passando pela primeira base, até

chegar à segunda - ou por um caminho que, no baseball, tiraria o bateador do jogo - passando pela terceira, até chegar à segunda.

Essa é a versão moderna do experimento da dupla fenda, é conduzida, agora, com divisores de feixes (*uma espécie de bifurcação na estrada ótica*). Existe um detector de luz que registra o impacto do fóton. Os caminhos que os fótons podem seguir, convergem de modo que a interferência de onda, se existe, pode ser detectada.

O divisor de feixes envia o fóton por uma das duas rotas, através da terceira ou primeira base, e o faz aleatoriamente, mas com probabilidades iguais de usar qualquer uma das rotas. Nessa variação, o detector de luz revela os padrões de interferência, assim como fez o experimento de dupla fenda. Os fótons estão agindo como ondas.

Agora, mudando o experimento um pouco. Posicione um detector de fótons por trás da primeira base ou da terceira. Um treinador (o técnico) sempre sabe quando um jogador passou por ele - ou se nenhum jogador passou por ele. Da mesma forma um detector de fótons pode determinar se um fóton passou ou não. Isso tem um efeito decisivo sobre o padrão de luz atrás da segunda base; o fóton agora é composto de duas faixas de luz, indicando que os fótons se comportam como partículas.

Objetos quânticos são notavelmente esquivos. Considere um fóton como exemplo. O quantum de luz (fóton) pode agir como partícula, seguindo um caminho bem definido como se fosse um minúsculo projétil; e no momento seguinte agir como uma onda, sobrepondo-se a outras para produzir padrões de interferência muito parecidos com ondulações na água.

A dualidade onda-partícula é uma característica fundamental da mecânica quântica, uma que não se compreende facilmente nos termos intuitivos da experiência cotidiana. Mas a natureza dupla de entidades quântico-mecânicas fica ainda mais estranha. Novos experimentos demonstram que fótons não apenas mudam de ondas para partículas, e de volta para ondas; mas que podem, na verdade, exibir tendências de ondas e partículas ao mesmo tempo. De fato, um fóton pode atravessar um complexo aparato ótico e desaparecer para sempre em um detector sem ter decidido sua identidade - assumindo uma natureza de onda ou partícula só depois de já ter sido destruído.

Há poucos anos, físicos mostraram que um fóton "escolhe" se quer agir como onda ou partícula quando é forçado a isso. Se, por exemplo, um fóton for enviado a um de dois caminhos por um *divisor de feixes*, e cada um desses caminhos levar a um **detector de fótons**, o fóton terá a mesma probabilidade de aparecer em qualquer um dos detectores. Em outras palavras, o fóton simplesmente escolhe uma das rotas e a segue com probabilidades iguais. Mas se os caminhos divididos se recombinarem-se antes dos detectores, permitindo que os conteúdos dos dois canais interfiram como ondas que se reencontram do outro lado, um fóton demonstra efeitos de interferência ondulatória, essencialmente passando pelos dois caminhos ao mesmo tempo. Se você mede um fóton como uma onda, ele age como uma. (STEIN, 2008)

## 4.5 Como os fótons sabem ?

Quando observados por um detector de fótons, esses (os fótons) se comportam como partículas. Quando não observados (quando não há detector de fótons), os

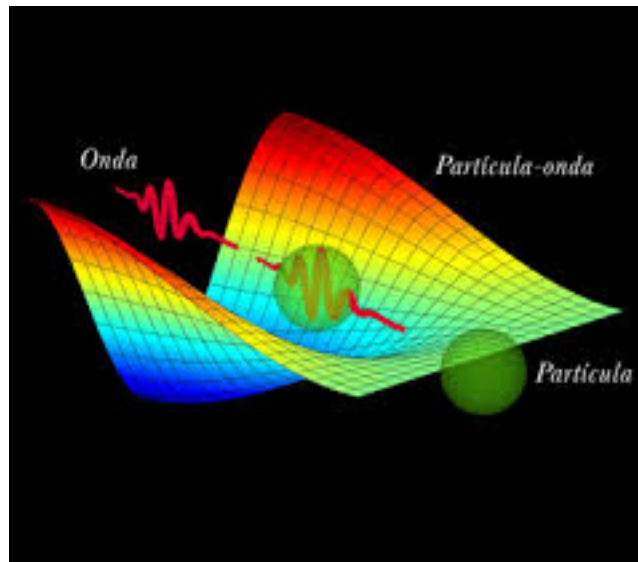


Figura 47 – A dualidade onda-partícula é uma característica fundamental da mecânica quântica.

Fonte: <[http://www2.uol.com.br/sciam/noticias/o\\_comportamento\\_dos\\_fotons\\_mostra\\_mais\\_surpresas.html](http://www2.uol.com.br/sciam/noticias/o_comportamento_dos_fotons_mostra_mais_surpresas.html)>

fótons se comportam como ondas. Isto é algo estranho. Veja na Figura 50. Mas, como é que um fóton sabe se está sendo observado ou não? Esse é um dos enigmas que estão no centro da mecânica quântica e, que aparece sob diferentes versões. A estranheza aumenta ainda mais. Na década de 70, **John Archibald Wheeler** propôs um experimento brilhante, conhecido como o *Experimento da Escolha Retardada*.

Posicione um detector de fótons bem longe da "última base" e, equipe-o com um interruptor de liga/desliga. Se o detector de fótons está ligado, os fótons se comportam como partículas; se estiver desligado, os fótons se comportam como ondas. Isto é, essencialmente, uma combinação dos dois experimentos anteriores (com detector ou sem detector). (STEIN, 2008)

A sugestão de **Wheeler** foi ligar ou desligar o detector de fótons depois de o fóton ter deixado a última base. Isto é conhecido como o **experimento da escolha retardada**, porque a escolha de ligar/desligar o detector é retardada até que o fóton tenha, presumivelmente, cumprido sua escolha entre se comportar como partícula ou como onda. Parece haver duas possibilidades - o comportamento do fóton é determinado no instante em que deixa a última base (mas, se for assim, como ele sabe se o detector está ligado ou desligado?), ou o comportamento do fóton é determinado pelo estado final do detector de fótons. Se a última hipótese for a correta (como de modo conclusivo, demonstrou-se pelos experimentos), o fóton deve simultaneamente estar em ambos os estados, quando deixa a última base, ou está num estado ambíguo que é resolvido ou quando passa pelo detector de fótons e aprende que está sendo observado, ou chega a segunda base sem ter sido observado.

Como foi previamente mencionado, a descrição matemática do fenômeno quântico é feita por meio de probabilidade. Um elétron, *antes de ser observado*, não tem uma posição definida no espaço, sua localização é definida por uma onda de probabilidade, que dá a probabilidade de que o elétron esteja localizado em certa





Figura 48 – John Weeler - Em 1970, o experimento da escolha retardada.

Fonte: <<http://www.manhattanprojectvoices.org>> (Google Images)



Figura 49 – John Weeler com Einstein -

Fonte: <<http://www.manhattanprojectvoices.org>> (Google Images)

porção do espaço. Antes de ser observado, o elétron está em todo lugar - embora seja mais provável que esteja em alguns lugares do que em outros. Além disso, ao se deslocar, usa todas as rotas possíveis disponíveis para tanto. Entretanto, o processo de observação "colapsa" a função de onda, de modo que o elétron não pode mais estar em todos os lugares, e, em vez disso permanece em algum lugar específico. A observação também quebra a capacidade do elétron de ir daqui para lá por todas as rotas possíveis e, em vez disso, seleciona uma rota dentre um número indeterminado muito grande de rotas possíveis.

**Wheeler** também propôs que a natureza podia ilustrar o quanto a mecânica quântica

é contra-intuitiva, por meio de um experimento grandioso de escolha retardada. Em vez de um divisor de feixes em um laboratório, um quasar a bilhões de anos-luz de distância, agindo como lente gravitacional, faria com que o divisor de feixes faz - permite que o fóton venha à Terra por um de dois caminhos diferentes. Esses caminhos deveriam ser focados no espaço; se nenhum detector de fótons fosse posicionado nesses caminhos, resultaria num padrão de interferência, e se houvesse detector de fótons colocados, os fótons agiriam como partículas. O aspecto contra-intuitivo é que o fóton, bilhões de anos atrás, quando passava pela lente gravitacional, parece ter tomado a decisão de agir como onda ou partícula. Experimentos mostram que essa decisão não é tomada pelo fóton, mas sim pelo universo - se uma observação é feita o fóton age como partícula; caso contrário, age como onda.

## 4.6 O Comportamento do fóton

Objetos quânticos são notavelmente esquivos. Alguns experimentos mostram o fóton como *partícula* ou como *onda* ao mesmo tempo. Tome um fóton, como exemplo. O *quantum* de luz (fóton) pode agir como *partícula*, seguindo um caminho bem definido como se fosse um minúsculo projétil; e no momento seguinte agir como uma *onda*, sobrepondo-se a outras para produzir padrões de interferência muito parecidos com ondulações na água.

A dualidade onda-partícula é uma característica fundamental da mecânica quântica, uma que não se compreende facilmente nos termos intuitivos da experiência cotidiana. Mas a natureza dupla de entidades quântico-mecânicas fica ainda mais estranha. Novos experimentos demonstram que fótons não apenas mudam de ondas para partículas, e de volta para ondas; mas que podem, na verdade, exibir tendências de ondas e partículas ao mesmo tempo. De fato, um fóton pode atravessar um complexo aparato ótico e desaparecer para sempre em um detector sem ter decidido sua identidade, assumindo uma natureza de onda ou partícula só depois de já ter sido destruído.

Há poucos anos, físicos mostraram que um fóton "escolhe" se quer agir como onda ou partícula quando é forçado a isso. Se, por exemplo, um fóton for enviado a um de dois caminhos por um divisor de feixes (uma espécie de bifurcação na estrada ótica), e cada um desses caminhos levar a um detector de fótons, o fóton terá a mesma probabilidade de aparecer em qualquer um dos detectores. Em outras palavras, o fóton simplesmente escolhe uma das rotas e a segue até o fim, como uma bolinha de gude em um tubo. Mas se os caminhos divididos se recombinarem antes dos detectores, permitindo que os conteúdos dos dois canais interfiram como ondas que fluem ao redor de um pilar e se reencontram do outro lado, um fóton demonstra efeitos de interferência ondulatória, essencialmente passando pelos dois caminhos ao mesmo tempo. Se você mede um fóton como uma onda, ele age como uma. (STEIN, 2008)

Pode-se suspeitar que os fótons simplesmente assumem um ou outro comportamento - onda ou partícula - com antecedência, ou quando atingem o divisor de feixes. Mas um experimento de 2007 sobre a "escolha retardada" eliminou essa possibilidade. Físicos usando um interferômetro, um dispositivo experimental que inclui o divisor de feixes, alternaram entre combinar os caminhos e mantê-los separados. Mas eles só decidiam entre um ou outro, depois de o fóton ter passado pelo divisor de ondas. Mesmo assim os fótons demonstraram efeitos de interferência quando recombinados, ainda que (pelo menos em um mundo simples) as partículas já devessem ter sido

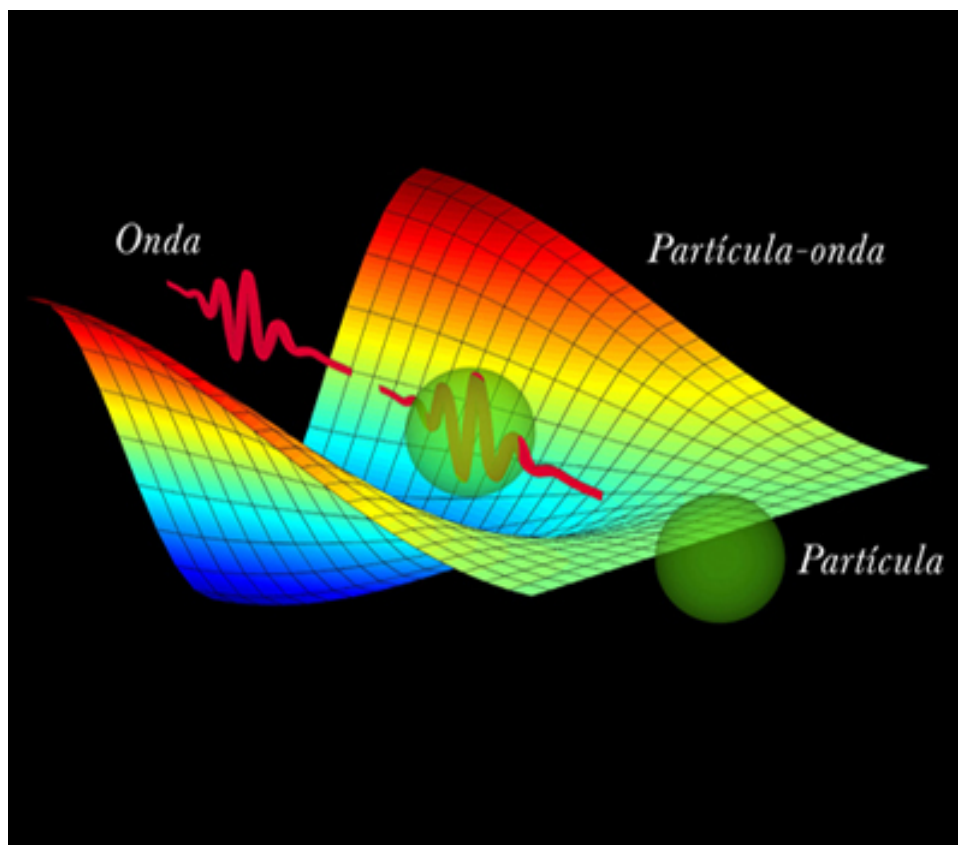


Figura 50 – Novos experimentos exploram a contínua transição de fótons agindo como partículas ou como ondas.

Fonte: <[http://www2.uol.com.br/sciam/noticias/o\\_comportamento\\_dos\\_fotons\\_mostra\\_mais\\_surpresas.html](http://www2.uol.com.br/sciam/noticias/o_comportamento_dos_fotons_mostra_mais_surpresas.html)>

forçadas a escolher qual caminho tomar.

Agora dois grupos de pesquisa utilizaram uma versão ainda mais bizarra do experimento de escolha retardada. Em dois estudos publicados em edição da *Nature*, uma equipe sediada na França e um grupo da Inglaterra relataram usar um interruptor quântico para modificar o dispositivo experimental. Exceto que, nesse experimento, o interruptor só foi ativado - assim forçando o fóton a agir como onda ou como partícula - depois que os físicos já haviam identificado o fóton em um dos detectores.

Ao mudar as configurações do dispositivo, as duas equipes não apenas conseguiram forçar o fóton experimental a se comportar como partícula ou onda, mas também conseguiram explorar estados intermediários. "Podemos mudar o comportamento do fóton de teste, de onda para partícula, continuamente", declara **Sébastien Tanzilli** (..), co-autor do estudo e físico especializado em ótica quântica do Centro Nacional de Pesquisas Físicas em Paris (CNRS), LPMC, Nice - **"Entre os dois extremos, nós temos estados que surgem com interferência reduzida. Então temos uma superposição de onda e partícula"**.

A chave dos dois experimentos é o uso de um interruptor quântico no aparato, que permite ao interferômetro ficar em superposição para medir comportamentos

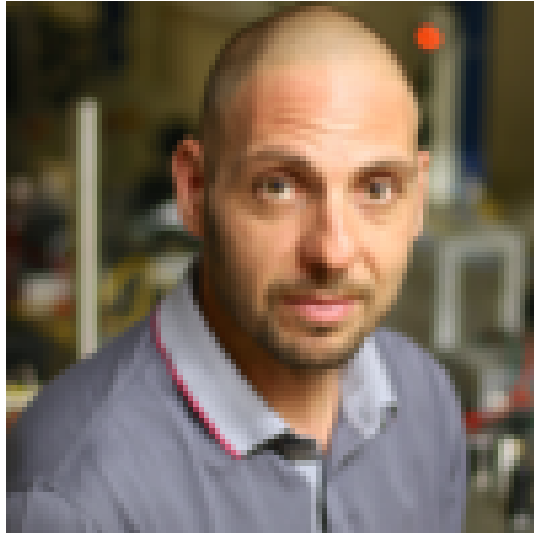


Figura 51 – Tanzilli - Entre os dois extremos, os estados que surgem da interferência.

Fonte: <<https://scholar.google.fr/citations?user=bHKWqpYAAAAJ&hl=en>>

ondulatórios ou particulados. "Nos tradicionais experimentos de escolha tardia, sempre há um grande interruptor binário clássico em algum lugar do aparato", explica **Peter Shadbolt** (1947-), coautor do outro estudo e aluno de doutorado em mecânica quântica da University of Bristol, na Inglaterra. "Ele tem 'onda' escrito de um lado e 'partícula' do outro. O que fazemos é substituir o interruptor clássico com um *qubit*, um *bit quântico*, que é um segundo fóton em nosso experimento".



Figura 52 – Peter Shadbolt - Substituindo o interruptor clássico por um bit quântico, que é um segundo fóton no experimento.

Fonte: <[hk.linkedin.com](https://www.linkedin.com/in/peter-shadbolt)> (Google Images)

O interruptor quântico determina a natureza do aparato - se os dois caminhos óticos se recombinam para formar um interferômetro fechado, que mede propriedades ondulatórias, ou se permanecem separados para formar um interferômetro aberto, que detecta partículas discretas. Mas em ambos os casos a abertura ou fechamento

do interferômetro - e a passagem do fóton pelo aparato como partícula ou onda, respectivamente - não era determinada até que os físicos medissem um segundo fóton. O destino do primeiro fóton estava ligado ao estado do segundo pelo fenômeno do emaranhamento quântico, em que objetos quânticos compartilham propriedades correlatas.

No experimento do grupo da University of Bristol, o estado do segundo fóton determina se o interferômetro está aberto, fechado, ou em uma superposição de ambos, o que por sua vez determina a identidade de partícula do primeiro fóton. "Em nosso caso, essa escolha está mais para uma escolha quântica", observa **Shadbolt**. "Sem esse tipo de abordagem, não seríamos capazes de ver essa transformação entre onda e partícula".

O dispositivo construído pelo grupo de **Tanzilli** funciona de maneira semelhante - o interferômetro fica fechado para fótons verticalmente polarizados (agem como ondas) e aberto para fótons horizontalmente polarizados (que se comportam como partículas). Tendo enviado um fóton de teste pelo aparato, os pesquisadores mediram um companheiro emaranhado do fóton 20 nanossegundos depois, para determinar a polarização do fóton de teste e assim identificar em qual dos lados da divisão *onda-partícula* ele estava.

Graças à estrutura do experimento e à natureza do emaranhamento, a natureza de onda ou partícula do fóton de teste só foi determinada quando o segundo fóton foi medido - em outras palavras, 20 nanossegundos depois do fato. "O fóton de teste nasce no interferômetro e é detectado, o que significa que é destruído", aponta **Tanzilli**. "Depois disso, determinamos seu comportamento". Essa ordem de operações leva o conceito de escolha tardia (retardada) ao extremo. "Isso significa que espaço e tempo parecem não ter qualquer papel nesse caso".

O pesquisador de informações quânticas **Seth Lloyd** (1960-...), do *Massachusetts Institute of Technology*, em um comentário para a *Scientific America Brasil* que acompanhava os dois artigos, batizou o fenômeno de "procrastinação quântica", ou "proquanstinação". "Na presença do emaranhamento quântico (no qual os resultados das medidas são mantidos juntos)", escreveu ele, "é possível evitar tomar uma decisão, mesmo se os eventos parecerem já terem feito isso".

Os novos experimentos adicionam outra ruga no estranho mundo da mecânica quântica, onde um fóton aparentemente pode ser o que quiser, quando quiser. **Richard Feynman** (1918-1988), foi um físico norte-americano do século XX, um dos pioneiros da eletrodinâmica quântica, e Nobel de Física de 1965. **Feynman** dizia que esse era o verdadeiro mistério da mecânica quântica. **Shadbolt** lembra, falando sobre a dualidade *onda-partícula*. "É profundamente, profundamente estranho. A mecânica quântica é profundamente estranha, completamente sem análogos clássicos, e tudo o que podemos fazer é aceitá-la assim".

A formulação de **Feynman** da mecânica quântica ou **formulação de integrais de caminho** da mecânica quântica é uma descrição da teoria quântica que generaliza a ação da mecânica clássica. Ela substitui a noção clássica de uma única trajetória para um sistema por uma soma ou integral funcional, por meio de uma infinidade de trajetórias possíveis para calcular a amplitude quântica (**FEYNMAN, 2010**). A ideia básica da formulação de *integral de caminho* é originária de **Norbert Wiener**, que apresentou o *processo para a solucionar problemas de difusão* e do *movimento Browniano* (**CHAICHIAN; DEMICHEV, 2001**).



Figura 53 – Seth Lloyd - O fenômeno da "procrastinação quântica".

Fonte: <[www.youtube.com](http://www.youtube.com)> (Google Images)



Figura 54 – Richard Feynman - A formulação de **Feynman** da mecânica quântica ou formulação de integrais de caminho da mecânica quântica.

Fonte: <[https://pt.wikipedia.org/wiki/Richard\\_Feynman](https://pt.wikipedia.org/wiki/Richard_Feynman)> (Google Images)

**Paul Adrien Maurice Dirac** (1902-1984) foi um físico teórico britânico. Estudou engenharia elétrica na Universidade de Bristol, completando o curso em 1921. Em 1923 graduou-se em matemática e recebeu uma bolsa de pesquisa no St John's College, na Universidade de Cambridge. Esta ideia da *integral de caminho* foi estendida por **Paul A. M. Dirac** (1902-1984), para o uso do *método lagrangiano* na mecânica quântica, em seu artigo de 1933 (**DIRAC, 1933**). O método completo foi desenvolvido em 1948 por **Richard Feynman**. Algumas preliminares foram trabalhados

anteriormente, no curso de sua tese de doutorado no trabalho de **John Archibald Wheeler**. A motivação original surgiu da aspiração de obter uma formulação da Mecânica Quântica para a Teoria de Ação à Distância de **Wheeler** e **Feynman** usando um operador *Lagrangiano* (ao invés de um operador **Hamiltoniano**) como ponto de partida.

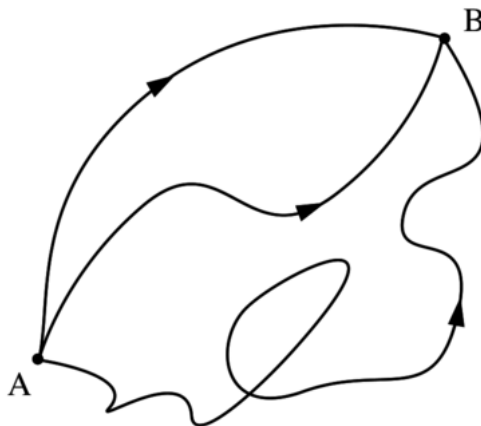


Figura 55 – Estes são apenas três dos caminhos que contribuem para amplitude quântica de uma partícula movendo-se do ponto A em tempo  $t_0$  para o ponto B em  $t_1$ .

Fonte: Google Images <<http://www.amath.washington.edu/~qian/gif/dirac.gif>>

## 4.7 Ondas de probabilidade e observações: Um exemplo humano

Embora possa parecer misteriosa a ideia de ondas de probabilidade e observações que as colapsam, há um análogo simples que ocorre anualmente em todas as universidades do país. Muitos estudantes entram como graduandos não declarados - incertos, onde está seu futuro, ou seja, em qual curso é mais adequado para sua vocação? Como resultado, frequentam vários cursos encorajados pela política geral e pedagógica da universidade, que requer que os alunos frequentem cursos em uma variedade de disciplinas. Esses estudantes são como ondas de probabilidade; suas especialidades, ainda não selecionadas, são um amálgama probabilístico de várias alternativas de cursos. (STEIN, 2008)

Em algum momento, contudo, o estudante deverá escolher sua especialização, o que normalmente é feita depois da conversa com um orientador, que apresenta ao aluno as opções disponíveis, os requisitos das várias especializações e os caminhos de carreira que cada uma delas abre (no caso do aluno ainda não saber), e o estudante faz sua escolha. Essa escolha colapsa a onda de probabilidade, e o estudante agora é um graduando declarado.

## 4.8 Você não é ninguém antes de ser observado

Na nossa vida real, isto é uma verdade. Na mecânica quântica, ocorre o mesmo. Você é considerado apenas uma onda de probabilidade, até você ser observado por

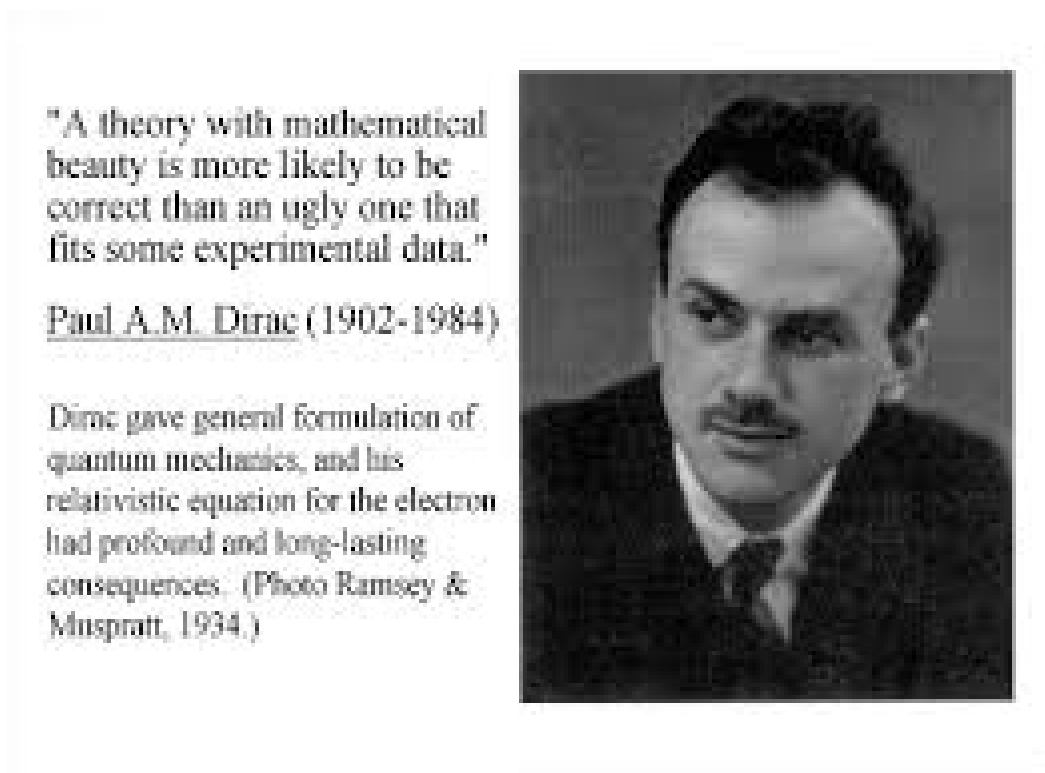


Figura 56 – Paul Dirac - A formulação da integral de caminho estendida para o método lagrangeano na mecânica quântica.

Fonte: Google Images <<http://www.amath.washington.edu/~qian/gif/dirac.gif>>

alguém, ou por algo. O que constitui uma observação no universo físico e quando ela se dá? Uma visão amplamente aceita na comunidade da Física é a de que uma observação consiste em uma interação com o universo. Nossa noção intuitiva de realidade - de que as coisas tem estados e atributos definidos - entra em colisão com o mundo apresentado pela mecânica quântica, no qual as coisas tem uma mistura probabilística de estados e atributos, e somente a interação com o universo pode criar uma realidade do que era inicialmente apenas uma possibilidade (STEIN, 2008).

## 4.9 O gato de Schrödinger

**Erwin Rudolf Josef Alexander Schrödinger** (1887-1961) foi um físico teórico austríaco, conhecido por suas contribuições à mecânica quântica, especialmente a equação de Schrödinger, pela qual recebeu o Nobel de Física em 1933. Ele lançou um modo de visualizar a esquisitice inerente ao comportamento quântico. Ele imaginou uma caixa contendo um gato, um frasco de gás venenoso e átomo radiotivo, que tem uma probabilidade de 50% de decair no espaço de tempo de 1 hora. Se decair, coloca em funcionamento um mecanismo que libera o gás venenoso, que pode matar o gato. Uma hora se passa. Em qual estado estará o gato?

A resposta convencional à pergunta é que o gato estará morto ou vivo, e descobriremos quando abrirmos a caixa. A mecânica quântica responde a esta questão dizendo que o gato está meio morto e meio vivo (ou que não está nem uma coisa nem outra), e a resposta sera conhecida quando a caixa for aberta.





Figura 57 – Erwin Schrödinger - O modo esquisito de visualizar o comportamento quântico.

Fonte: <[https://es.wikipedia.org/wiki/Erwin\\_Schrödinger](https://es.wikipedia.org/wiki/Erwin_Schrödinger)>

Não importa quão contra-intuitivo o gato meio-morto, meio-vivo possa ser, essa é a interpretação que a mecânica quântica dá - e como podemos refutá-la? Sem uma observação (que não necessariamente consiste em examinar o gato, mas simplesmente em obter informações sobre o estado átomo radioativo cuja decadência determina o resultado), como poderemos saber?

Como método computacional, a mecânica quântica provavelmente é o mais exato na Física. A alguns físicos parece que isso é tudo o que a Física pode fazer - prover regras de cálculo que nos permitem construir computadores ou aparelhos de ressonância magnética. Um número bem maior de físicos pensa que isso nos diz algo profundo e importante sobre a realidade. Mas a comunidade da Física ainda não chegou a um consenso sobre o que seja a realidade. (STEIN, 2008)

## 4.10 Apagadores quânticos

A ideia de que fótons e elétrons são ondas de probabilidade até que sejam observados, momento em que viram partículas (STEIN, 2008), tem sido assunto de inúmeros experimentos. Um tipo especialmente engenhoso de experimento é o do *apagador quântico*, concebido inicialmente por **Marlan Scully** (1939-) e **Kai Druhl** (..) em 2000. Ver **Kai Druhl** em <<http://www.thetrueight.net/personalstories/kaidruhl.htm>>

**Marlan Orvil Scully** é um físico estadunidense. É conhecido por seu trabalho



Figura 58 – Marlan Scully - O experimento do apagador quântico, concebido juntamente com Kai Druhl.

Fonte: Google Images

em óptica quântica teórica. É atualmente professor da Texas A&M University e da Universidade de Princeton.



Figura 59 – Kai Druhl - O experimento do apagador quântico, concebido juntamente com **Marlan Scully**.

Fonte: Google Images in <[www.twitter.com](http://www.twitter.com)>

Voltando à versão "beisebolística", imaginemos que quando um fóton passa por um dos técnicos, o técnico lhe dá um tapa nas costas (não muito diferente de um técnico de baseball real), colando um rótulo identificador que nos habilita a saber qual rota o fóton usa. Quando isso acontece, claramente faz-se uma *observação*, e o fóton age como partícula - o padrão do detector atrás da segunda base são as já conhecidas duas manchas que caracterizam as partículas.

Agora suponha que, de algum modo, assim como os fótons rotulados chegam à segunda base, os rótulos são removidos (essa rotulação e desrotulação de fótons, há um meio de fazer isto, mas os detalhes não importam para esta discussão). Deixa de haver, então, a evidência da rotulação - os rótulos foram apagados (daí o termos apagadores quânticos). Não havendo evidência de qual caminho os fótons usaram para chegar à segunda base, o padrão de *interferência* reerge.

Esse foi exatamente o resultado previsto por **Marlan Scully** e **Kai Druhl**. Entendemos **o que a Mecânica Quântica está nos dizendo: que fótons e elétrons são ondas de probabilidade até que interajam com o universo, quando então viram partículas**. Se não podemos determinar se eles, de fato, interagiram com o universo - e é isso que o apagador quântico realiza - eles são ondas de probabilidade. Dentre as coisas que jamais poderemos conhecer é o porquê de isso ser assim, e se poderia ser de outra maneira. Este é um dos objetivos de longo prazo da Física: dizer-nos não só como é o universo, mas porque este é o único modo possível - ou se poderia ser de alguma outra forma. (STEIN, 2008)

## 4.11 O princípio da incerteza

Alguns ramos da Matemática, como por exemplo, a Geometria, são altamente visuais. Outros, como a Álgebra, são altamente simbólicos, embora muitos resultados importantes tenham sido obtidos ao se olhar geometricamente para problemas algébricos ou algebricamente para problemas geométricos. Entretanto, a maioria das pessoas tem uma preferência por olhar as coisas de uma forma ou de outra.

**Einstein** tinha um belo jeito de expressar isso: em seus últimos anos, ele observou que pouquíssimas vezes pensara em Física usando palavras. Era possível que ele visse figuras; talvez até mesmo relações entre conceitos. Pensar em figuras, são quase sempre derivadas das palavras que as descrevem.

À medida que a Física investigava cada vez mais a fundo o mundo subatômico nas primeiras décadas do século XX, tornou-se cada vez mais difícil visualizar os fenômenos estudados. Como resultado, alguns físicos - incluindo **Werner Heisenberg** - preferiram tratar o mundo subatômico somente por representações simbólicas. **Werner Heisenberger** (1901-1976), foi um físico alemão, ganhador do Prêmio Nobel de Física em 1932, por suas contribuições à mecânica quântica.

Ele se tornou um dos assistentes de **Niels Bohr**. **Heisenberg** ganhou familiaridade com o modelo do átomo de **Bohr**, nos quais elétrons eram vistos como orbitando em seu núcleo.

Naquela época o modelo de **Bohr** encontrava certas dificuldades teóricas, e vários físicos se dedicavam a sua resolução. Um deles era **Erwin Schrödinger**. A solução de **Schrödinger** tratava o mundo subatômico como composto de ondas, em vez de partículas. **Heisenberg** adotou uma abordagem diferente. Ele concebeu um modelo



Figura 60 – Heisenberg em 1933 - O princípio da incerteza da mecânica quântica.

Fonte: <[https://pt.wikipedia.org/wiki/Werner\\_Heisenberg](https://pt.wikipedia.org/wiki/Werner_Heisenberg)>

matemático composto por matrizes que podiam ser manipuladas de tal maneira a gerar resultados experimentais conhecidos. As abordagens de **Schrödinger** e **Heisenberg** funcionavam, já que davam conta de mais fenômenos do que o modelo atômico de **Bohr**. Mais tarde mostrou-se que ambas as teorias eram equivalentes, gerando os mesmos resultados com o uso de diferentes ideias.

Em 1927, **Heisenberg** estava prestes a fazer a descoberta que não só lhe daria o Prêmio Nobel, como também mudaria para sempre o panorama filosófico sobre a teoria quântica.

*Determinismo* é a teoria filosófica de que todo acontecimento (inclusive o mental) é explicado pela *determinação*, ou seja, por *relações de causalidade*. O matemático francês **Pierre Laplace** (1749-1827) acreditava fortemente no determinismo. No final do século XVIII, **Laplace** enunciou a quintessência do determinismo científico, afirmando que, ao saber a posição e o momento (produto de sua massa por sua velocidade) de cada objeto do universo, seria possível calcular exatamente onde cada objeto estaria em todos os instantes futuros. **Laplace** dizia "*Nós podemos tomar o estado presente do universo como o efeito do seu passado e a causa do seu futuro ...*". Enquanto **Laplace** via primeiramente problemas práticos para que a humanidade atingisse tal estado final de conhecimento e computação, interpretações da mecânica quântica posteriores, foram adotadas por filósofos. A teoria das probabilidades é o estudo matemático das probabilidades de que eventos venham a ocorrer. **Pierre Simon Laplace** é considerado o fundador da Teoria das Probabilidades.

O **princípio da incerteza de Heisenberg** declara - *que tanto é impossível saber*



Figura 61 – Niels Bohr em 1922 - O modelo de átomo nos quais elétrons eram vistos como orbitando seu núcleo.

Fonte: <[https://pt.wikipedia.org/wiki/Niels\\_Bohr](https://pt.wikipedia.org/wiki/Niels_Bohr)>

*exatamente onde qualquer coisa está, quanto para onde está indo em qualquer instante determinado.*

Essas dificuldades, na verdade, não se manifestam no mundo macroscópico - se alguém joga uma bola de boliche em sua direção, você normalmente consegue prever a posição futura da bola de boliche e, quem sabe até manobrar para sair da frente dela. Por outro lado, se tanto você quanto a bola de boliche forem do tamanho de elétrons, você terá problemas em descobrir para que lado se mover, pois não vai saber para onde está indo a bola de boliche microscópica.

Podemos entender algo da ideia subjacente no princípio da incerteza de **Heisenberg** olhando para um acontecimento cotidiano - a compra de combustível em um posto. O custo da transação consiste em um número de reais e centavos até sua terceira casa decimal - o centavo e quantum de nosso sistema monetário, a menor unidade irredutível da moeda. O custo é calculado, arredondando-se até o centavo mais próximo, e isso torna impossível para determinarmos com precisão quanto combustível foi de fato comprado, mesmo que saibamos o preço exato do litro do combustível, por exemplo, R\$3,099. (STEIN, 2008)

*... Quanto menor o custo do combustível, maior será a incerteza posicional.*

O **princípio da incerteza de Heisenberg** opera de acordo com linhas parecidas. Ele declara que o produto das incertezas de duas variáveis relacionadas, chamadas



Figura 62 – Laplace - O estado presente do universo como o efeito do seu passado e a causa do seu futuro ...

Fonte: <[https://pt.wikipedia.org/wiki/Pierre-Simon\\_Laplace](https://pt.wikipedia.org/wiki/Pierre-Simon_Laplace)>

**variáveis conjugadas**, deve ser maior do que alguma quantidade fixa predeterminada. Possivelmente as variáveis conjugadas mais conhecidas sejam a duração de uma nota musical e sua frequência - quanto mais tempo a nota for sustentada, com mais exatidão poderemos determinar sua frequência. Uma nota tocada por um período infinitesimalmente pequeno de tempo, tem simplesmente o som de um clique; e assim é impossível determinarmos sua frequência.

No entanto, o detalhe problemático do princípio da incerteza é o fato de que a *posição* e o *momento* (momento é o produto de massa e velocidade) são variáveis conjugadas. Quanto mais acuradamente pudermos definir a *posição* de uma partícula, menos informações teremos sobre seu *momento*. E se pudermos determinar seu momento com alto grau de exatidão, teremos somente uma noção limitada de onde a partícula está. Como momento é produto de massa e velocidade, uma quantidade microscópica de *momento* que resultaria numa velocidade quase nula no caso de um automóvel, resulta numa grande velocidade no caso de um elétron.

O **princípio da incerteza de Heisenberg** é uma declaração sobre as limitações do conhecimento, e uma consequência direta da visão que a mecânica quântica tem do mundo. Como parte fundamental da mecânica quântica, o **princípio da incerteza de Heisenberg** tem ramificações no mundo real para a construção de itens do dia-a-dia, tais como lasers e computadores. Ele banuiu a simples perspectiva de causa e efeito do universo, que se mantivera sem questionamentos desde a sua primeira enunciação pelos filósofos gregos. (STEIN, 2008)

Formulando sobre uma das consequências do princípio da incerteza, **Heisenberg**

dizia:

"... ... *Nos experimentos sobre eventos atômicos temos de lidar com coisas e fatos, com fenômenos que são tão reais quanto qualquer fenômeno da vida diária. Mas os próprios átomos ou partículas elementares não são tão reais; eles formam um mundo de potencialidades ou possibilidades, e não um mundo de coisas ou fatos ... .*  
*Átomos não são coisas.*"

Se átomos não são coisas, o que são então? Mais de 85 anos depois da revelação de **Heisenberg**, físicos e filósofos, ainda lutam com essa questão. A resposta que achamos anteriormente, de que átomos são ondas de probabilidade até que sejam observados e, depois disso, coisas, não são inteiramente satisfatória, mas é o melhor que poderemos fazer até agora.

## 4.12 Emaranhamento e o experimento EPR de Einstein, Podolsky e Rosen

Muitas propriedades da mecânica quântica são parecidas como o dilema *onda-partícula* engendrado pelos *fótons* - até que uma medição seja feita a propriedade existe em uma superposição de várias possibilidades diferentes. Uma dessas propriedades é a rotação em torno de um eixo. Um *fóton* pode girar para a esquerda ou para a direita, em torno de um eixo, uma vez que aquele eixo seja selecionado e o *fóton* observado, mas terá um *spin* para a esquerda 50% das vezes e, para a direita, outros 50% das vezes, e fará isso de modo aleatório. Mas, na mecânica quântica não faz sentido dizer que uma partícula "gira" em torno de um eixo. Esta é apenas uma imagem para se estabelecer uma analogia com algo mais familiar. Essa propriedade é chamado *spin* da partícula, termo inglês usado internacionalmente. (STEIN, 2008)

O que é o *spin* de uma partícula? O *spin* é uma propriedade intrínseca da mesma, assim como sua massa e sua carga elétrica. Dizemos que o *spin* é um número quântico das partículas. O número quântico  $s$  é um número inteiro e é denominado de número quântico de *spin*. É uma constante fundamental da teoria quântica.

Quando um átomo de cálcio emite energia e, mais tarde volta ao seu estado inicial, emite dois fótons. Diz-se que os fótons estão emaranhados - o resultado da medição do *spin* de um *fóton* automaticamente determina o resultado do *spin* do outro *fóton*, muito embora, inicialmente, nenhum *fóton* possua um *spin* definido, mas apenas uma *onda de probabilidade* que deixa espaço igual para *spins* à esquerda ou à direita. Ao menos, esse é um ponto de vista amplamente aceito pelos físicos.

**Einstein** ficava extremamente inquieto diante dessa perspectiva, e então, junto com os físicos **Boris Podolsky** e **Nathan Rosen** desenvolveu um experimento hipotético, conhecido como o experimento EPR (vem das iniciais de **Albert Einstein**, **Boris Podolsky** e **Nathan Rosen**), que desafiava aquela ideia. **Einstein**, **Podolsky** e **Rosen** faziam objeção à ideia de que, antes das medições, nenhum *spin* é conhecido.

Esta versão do experimento ERP foi trabalhada pelo estadunidense **David Bohm** (1917-1992), que foi professor da University of Princeton, mas posteriormente, veio para o Brasil trabalhar na USP (Universidade do Estado de São Paulo) entre 1951 e

1955. **David Bohm** converteu o experimento mental inicial em algo próximo a um experimento viável.



Figura 63 – David Bohm - Converteu o experimento ERP mental inicial em algo próximo a um experimento viável.

Fonte: <[https://en.wikipedia.org/wiki/David\\_Bohm](https://en.wikipedia.org/wiki/David_Bohm)> ,

A reinterpretação da teoria quântica proposta por **David Bohm** - O interesse de **David Bohm** pelos fundamentos da teoria quântica não esgotou-se na redação do seu livro *Quantum Theory*. Concluído o texto ele enviou-o a **W. Pauli**, **N. Bohr** e **A. Einstein**. **Pauli** manifestou-se elogiando o conteúdo, mas **Bohr** não respondeu. **Einstein**, que trabalhava em Princeton, convidou-o para discussões quando expôs sua própria apreciação a respeito desta teoria. Estas discussões contribuíram para motivar **Bohm** a buscar uma nova abordagem para estes problemas. O trabalho publicado em 1952 consiste na construção de um modelo físico capaz de reproduzir todos os resultados que podem ser obtidos com a teoria quântica, na sua interpretação usual, mas apoiado em um "quadro conceitual mais amplo" que, com o auxílio de parâmetros adicionais (ocultos), "permite uma descrição contínua, detalhada e causal de todos os processos", mesmo no nível quântico. O leitor pode ler sobre **David Bohm** em <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0103-40141994000100012](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40141994000100012)> .

**Albert Einstein** foi um físico teórico alemão. Entre seus principais trabalhos desenvolveu a *teoria da relatividade* geral, ao lado da mecânica quântica um dos dois pilares da Física moderna.

**Boris Podolsky** (1896-1966) foi um físico russo que imigrou para os Estados Unidos. Trabalhou com **Albert Einstein** e **Nathan Rosen** e concebeu o *Paradoxo EPR*, que é de máxima importância para a Física quântica.

**Nathan Rosen** (1909-1995) foi um físico estadunidense naturalizado israelense.



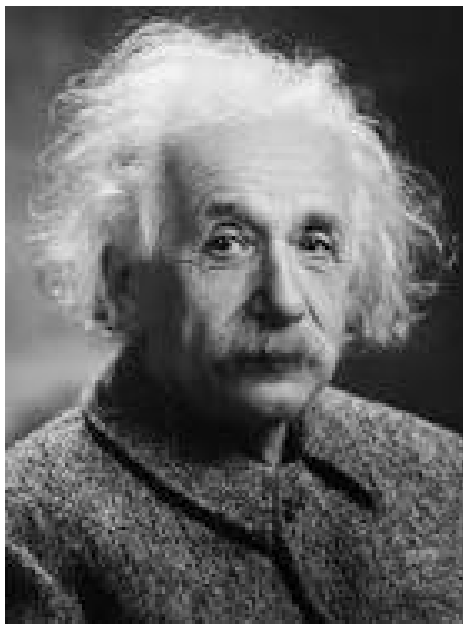


Figura 64 – Albert Einstein em 1947 - Juntamente com Podolsky e Rose imaginaram o experimento ERP.

Fonte: <[https://en.wikipedia.org/wiki/Albert\\_Einstein](https://en.wikipedia.org/wiki/Albert_Einstein)>



Figura 65 – Boris Podolsky - Juntamente com Einstein e Rose imaginaram o experimento ERP.

Fonte: <[https://en.wikipedia.org/wiki/Boris\\_Podolsky](https://en.wikipedia.org/wiki/Boris_Podolsky)>

É conhecido por seus estudos sobre a estrutura da molécula de hidrogênio e seu trabalho com **Albert Einstein** e **Boris Podolsky** resultando no paradoxo EPR (Einstein-Podolsky-Rosen).



Figura 66 – Nathan Rose - A estrutura da molécula de hidrogênio, e juntamente com Einstein e Podolsky imaginou o experimento ERP.

Fonte: <[https://en.wikipedia.org/wiki/Nathan\\_Rose](https://en.wikipedia.org/wiki/Nathan_Rose)>

Suas contribuições para a Física, principalmente na área da mecânica quântica, foram significativas. Seu primeiro livro, *Teoria Quântica*, publicado em 1951, foi considerado por **Einstein** a exposição mais clara que ele já havia visto sobre o assunto. Insatisfeito com a abordagem ortodoxa da Física Quântica descrita por ele neste mesmo livro, desenvolveu sua própria interpretação, uma *teoria determinística da variável oculta não-local* cujas previsões concordam perfeitamente com as *teorias quânticas não-determinísticas*. Seu trabalho foi um dos motivadores da desigualdade de Bell, cujas consequências ainda estão sendo investigadas.

O EPR surgiu em meio a um contexto histórico onde buscava-se, em vista das previsões da mecânica quântica, a compreensão da realidade adjacente a uma partícula descrita por um *estado emaranhado*. **O EPR é um paradoxo no seguinte sentido: tomando-se a mecânica quântica e a ela adicionando-se uma condição aparentemente razoável - tal como "localidade", "realismo" ou "inteireza - presentes em outras teorias como a clássica ou relativística, obtém-se uma contradição.** Porém, a mecânica quântica por si só não apresenta nenhuma inconsistência interna, tão pouco deixa indícios de como estas poderiam sugerir; também não contradiz a teoria relativística de **Einstein** ou mesmo a mecânica clássica de **Newton**; e mais, implica esta última no limite macroscópico - quando tem-se agregados de numerosas partículas. Ver em <[https://pt.wikipedia.org/wiki/Paradoxo\\_EPR](https://pt.wikipedia.org/wiki/Paradoxo_EPR)>.

O **entrelaçamento quântico** (ou **emaranhamento quântico**, como é mais conhecido na comunidade científica) **é um fenômeno da mecânica quântica que permite que dois ou mais objetos estejam de alguma forma tão ligados que um objeto não possa ser corretamente descrito sem que a sua contra-parte seja mencionada - mesmo que os objetos possam estar espacialmente separados por milhões de anos-luz.** Isso leva a correlações muito fortes entre as propriedades físicas observáveis das diversas partículas subatômicas.

Essas fortes correlações fazem com que as medidas realizadas numa delas pareçam estar a influenciar instantaneamente à outra com a qual ficou entrelaçada, e sugerem que alguma influência estaria a propagar-se instantaneamente, apesar da separação entre eles. Mas o entrelaçamento quântico não permite a transmissão a uma velocidade superior à da velocidade da luz, porque nenhuma informação útil pode ser transmitida desse modo. Só é possível a transmissão de informação usando um conjunto de estados entrelaçados em conjugação com um canal de informação clássico - aquilo a que se chama o teletransporte quântico. Isto dá a entender que tudo está conectado por "forças" que não vemos e que permanecem no tempo, ou estão fora do sistema que denominamos, entendemos ou concebemos como sistema temporal.

O *entrelaçamento quântico* é a base para tecnologias emergentes, tais como **computação quântica**, **criptografia quântica** e tem sido usado para experiências como o **teletransporte quântico**. Ao mesmo tempo, isto produz alguns dos aspectos teóricos e filosóficos mais perturbadores da teoria, já que as correlações previstas pela mecânica quântica são inconsistentes com o princípio intuitivo do realismo local, que diz que cada partícula deve ter um estado bem definido, sem que seja necessário fazer referência a outros sistemas distantes. Os diferentes enfoques sobre o que está a acontecer no processo do entrelaçamento quântico dão origem a diferentes interpretações da mecânica quântica.

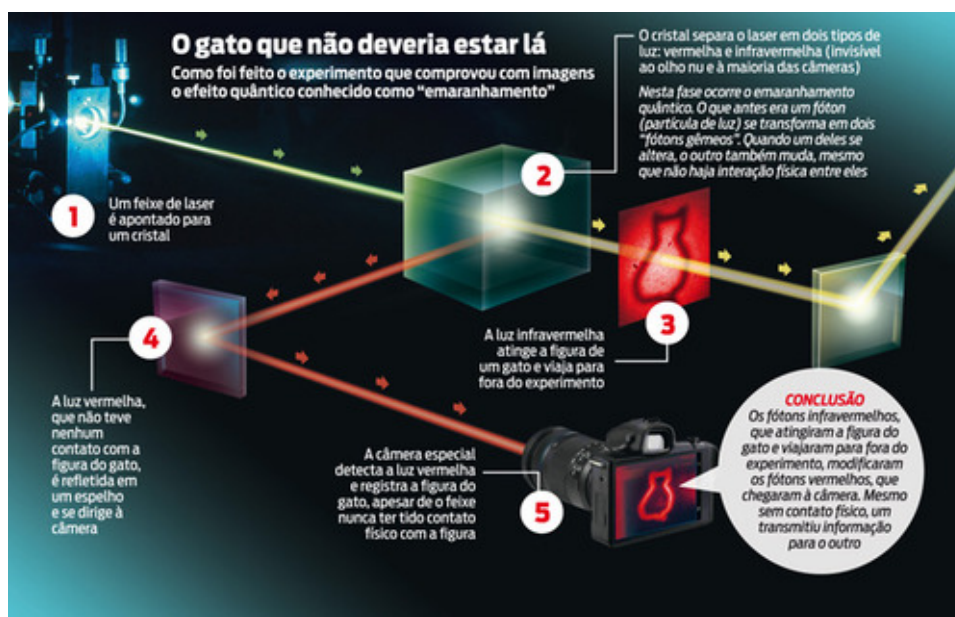


Figura 67 – O experimento que comprovou com imagens, o efeito quântico conhecido como emaranhamento/entrelaçamento quântico. Múltiplas partículas estão ligadas entre si de uma forma tal que a medição do estado quântico de uma partícula determina os possíveis estados quânticos das outras partículas.

Fonte: Google Images

### 4.12.1 Exemplo clássico de Emaranhamento Quântico

O exemplo clássico de entrelaçamento quântico é chamado o paradoxo EPR ou (**Einstein, Podolsky e Rosen**). Em uma versão simplificada deste caso, considere uma partícula quântica com rotação 0 que se decompõe em duas novas partículas, partículas A e B. Cada partícula, A e B, encabeçam em direções opostas. No entanto, a partícula original tinha um spin quântico 0. Cada uma das novas partículas tem um spin quântico  $1/2$ , mas, como elas têm que se somar e resultar a 0, uma deve ser  $+1/2$  e outra,  $-1/2$ .

Esta relação significa que as duas partículas estão emaranhadas. Quando você mede o spin das Partículas A, a medida tem um impacto sobre os possíveis resultados que você poderia ter quando medisse o *spin* da partícula B. E isso não é apenas uma previsão teórica interessante, mas foi verificada experimentalmente através de testes de Teorema de Bell.

Uma coisa importante a lembrar é que, na física quântica, a incerteza inicial sobre o estado quântico da partícula não é apenas uma falta de conhecimento. A propriedade fundamental da teoria quântica é que, antes do ato de medir, a partícula realmente não tem um estado definitivo, mas é em uma superposição de todos os estados possíveis. **O princípio da superposição é a ideia de que um sistema está em todos os estados possíveis ao mesmo tempo, até que seja medido. Após a medição, ele cai em um dos estados base que formam a superposição, destruindo assim a configuração original.** Este é o que é melhor modelado pelo experimento mental quântico clássico da Física, o gato de **Schrödinger**, onde a abordagem da mecânica quântica resulta em um gato não observado que está vivo e morto ao mesmo tempo. **Einstein** chamou isso de *efeito fantasmagórico à distância*. (STEIN, 2008)

## 4.13 EPR, o Estado Emaranhado e as Variáveis Ocultas

**Einstein, Podolsky e Rosen** foram os três defensores do ponto de vista realista que apresentaram este experimento mental em um trabalho de 1935, no intuito de demonstrar que *a mecânica quântica não é uma teoria física completa*, faltando à *função de onda* que descreve o *estado emaranhado* o que eles chamaram de "variáveis ocultas", com as quais seria possível restaurar-se a explicação estritamente realista que defendiam.

Suponha que dois grupos de experimentadores, anos-luz distantes um do outro, decidissem medir os spins desses fótons. Se o spin do fóton A é medido e, segundos depois, o spin do fóton B é medido, a mecânica quântica prevê que o fóton B "saberia" o resultado da medição do spin do fóton A, mesmo não havendo tempo suficiente para que um sinal do fóton A alcançasse o fóton B, e informasse o fóton B de como deve ser seu spin!

De acordo com **Einstein**, duas escolhas restavam. Era possível aceitar a chamada *Interpretação de Copenhagen* da mecânica quântica, que se deve a **Niels Bohr**, no sentido de que o fóton B saberia o que aconteceu ao fóton A, mesmo sem que uma comunicação ocorra entre eles. Alternativamente, poder-se-ia acreditar que existe uma realidade mais aprofundada, manifestada em alguma propriedade física ainda não encontrada nem medida, que explicaria esse fenômeno. **Einstein** faleceu

firmemente apegado a esse segundo ponto de vista, que é conhecido na comunidade da Física como "*variáveis ocultas*". (STEIN, 2008)

#### 4.13.1 A Interpretação de Copenhagen

A *Interpretação de Copenhagen* é a interpretação mais comum da mecânica quântica e foi desenvolvida por **Niels Bohr** e **Werner Heisenberg** que trabalhavam juntos em Copenhagen (Dinamarca) em 1927. Pode ser condensada em três teses:

- As previsões probabilísticas feitas pela mecânica quântica são irredutíveis no sentido em que não são um mero reflexo da falta de conhecimento de hipotéticas variáveis escondidas. No lançamento de dados, usamos probabilidades para prever o resultado porque não possuímos informação suficiente apesar de acreditarmos que o processo é determinístico. As probabilidades são utilizadas para completar o nosso conhecimento. A *interpretação de Copenhagen* defende que em Mecânica Quântica, os resultados são *indeterminísticos*.
- A Física é a ciência dos resultados de processos de medida. Não faz sentido especular para além daquilo que pode ser medido. A *interpretação de Copenhagen* considera sem sentido, perguntas como "onde estava a partícula antes da sua posição ter sido medida?".
- O ato de observar provoca o "*colapso da função de onda*", o que significa que, embora antes da medição o estado do sistema permitisse muitas possibilidades, apenas uma delas foi escolhida aleatoriamente pelo processo de medição, e a *função de onda* modifica-se instantaneamente para refletir essa escolha.

A complexidade da mecânica quântica foi atacada pela experiência (imaginária) de **Einstein-Podolsky-Rosen**, que pretendia mostrar que têm que existir variáveis ocultas para evitar "*efeitos não locais e instantâneos à distância*". As *desigualdades de Bell* sobre os resultados de uma tal experiência foi derivada do pressuposto de que *existem variáveis ocultas* e não existem "*efeitos não-locais*". Em 1982, **Alain Aspect** () levou a cabo a experiência e descobriu que as *desigualdades de Bell* eram violadas, rejeitando interpretações que postulavam variáveis ocultas e efeitos locais. Esta experiência foi alvo de várias críticas e novas experiências realizadas por **Weih** e **Rowe** confirmaram os resultados de **Aspect**.

**Alain Aspect** (1947-) é um físico francês conhecido como o primeiro físico a conduzir testes experimentais conclusivos sobre o paradoxo EPR. Os experimentos de Aspect foram considerados uma prova incontestável para suportar a teste que *desigualdades de Bell* foram violadas.

Muitos físicos e filósofos notáveis têm criticado a *Interpretação de Copenhagen*, com base, quer no fato de *não ser determinística*, quer no fato de propor que a *realidade é criada por um processo de observação não físico*. **Einstein** ilustra a posição dos críticos. A experiência do *Gato de Schroedinger* foi proposta para mostrar que a *Interpretação de Copenhagen* é absurda. A alternativa principal à *Interpretação de Copenhagen* é a *Interpretação dos Muitos Mundos* de **Hugh Everett**.

#### 4.13.2 A Interpretação dos Muitos Mundos

A *Interpretação de Muitos Mundos* (ou IMM) é uma interpretação da mecânica quântica que propõe a existência de múltiplos "universos paralelos". A IMM foi



Figura 68 – Alain Aspect em Tel-Aviv University aos 70 anos - Em 1982, ele descobriu que as *desigualdades de Bell* eram violadas.

Fonte: <[https://en.wikipedia.org/wiki/Alain\\_Aspect](https://en.wikipedia.org/wiki/Alain_Aspect)>

formulada inicialmente por **Hugh Everett** para a explicação de alguns processos não determinísticos (tais como medição) na mecânica quântica. Embora varias versões de IMM tenham sido propostas desde o trabalho original de **Everett**, todas compartilham duas ideias-chave:

- A primeira delas é a existência de uma função estado para todo universo a qual obedece à equação de Schrödinger para todo tempo e para a qual não há processo de colapso da onda.
- A segunda ideia é que este estado universal é uma sobreposição quântica de vários, possivelmente infinitos, estados de idênticos universos paralelos não comunicantes.

**Hugh Everett** (1930-1982) foi um físico estadunidense que propôs a interpretação de muitos mundos (IMM) da física quântica, que ele chamou formulação do "estado relativo". As ideias da IMM originaram-se na tese de Ph.D. de **Hugh Everett** na Universidade de Princeton, mas a frase "muitos mundos" é devida a **Bryce DeWitt** (1923-2004), um físico teórico estadunidense que posteriormente desenvolveu algumas das ideias presentes no trabalho original de **Hugh Everett**, que avançou na sua formulação original. A formulação de **Bryce DeWitt** tornou-se tão popular que muitos confundem-na com o trabalho original de **Everett**. IMM é uma das muitas hipóteses de multiversões na Física e na Filosofia.



Figura 69 – Hugh Everett - A interpretação da mecânica quântica que propõe a existência de múltiplos "universos paralelos".

Fonte: <[https://en.wikipedia.org/wiki/Hugh\\_Everett](https://en.wikipedia.org/wiki/Hugh_Everett)>

#### 4.14 O Teorema de Bell

Mais de uma centena de artigos foi escrita entre 1935 e 1964, discutindo os prós e contras à hipótese das *variáveis ocultas*, mas eram apenas discussões e argumentos - até que o físico irlandês **John Bell** veio com um experimento, que colocaria verdadeiramente em teste à teoria das *variáveis ocultas*.

Como um resultado de desenvolvimentos teóricos e experimentais seguintes ao trabalho original do EPR - destaca-se o *Teorema de Bell* (publicado em meados de 1960) e os resultados experimentais oriundos da investigação deste - demonstrou-se que se a visão realista estivesse correta ela implicaria não apenas a mecânica quântica como uma teoria incompleta, mas sim, como um teoria completamente incorreta, e por outro lado, se a mecânica quântica estivesse correta, então nenhuma variável oculta seria capaz de salvar a *teoria da não-localidade*, que **Einstein** considerava tão absurda. Restava decidir-se pela posição realista ou ortodoxa.

**John Stewart Bell** (1928-1990) foi um físico que se tornou conhecido como o criador do *Teorema de Bell*, apontado por alguns na comunidade da física quântica como uns dos teoremas mais importantes do século 20. (STEIN, 2008)

Em 1964, um ano após ter deixado o CERN (o qual passou na Universidade de Stanford, Universidade de Wisconsin e Universidade Brandeis), ele deduziu o seu famoso *Teorema de Bell*, concluindo que **nenhuma teoria de variáveis locais ocultas poderia ser válida no contexto da mecânica quântica**.

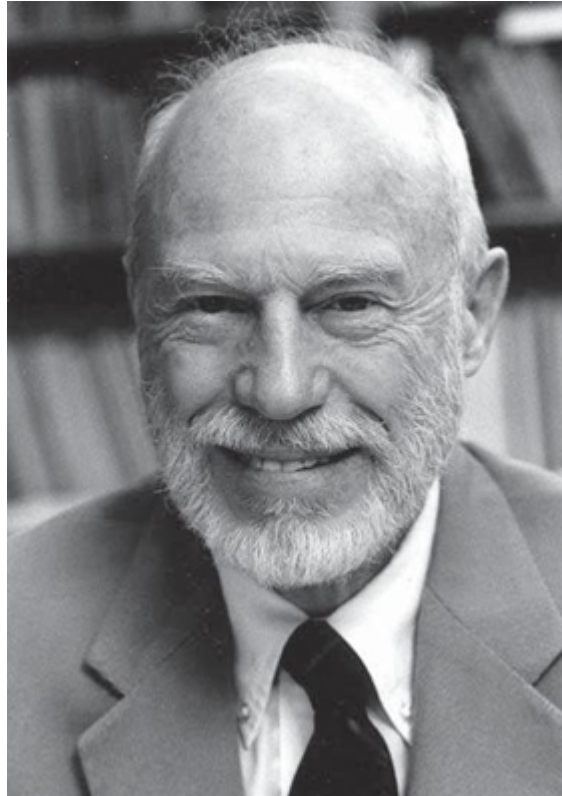


Figura 70 – Bryce DeWitt - Quem desenvolveu algumas das ideias presentes no trabalho original de **Hugh Everett**.

Fonte: <[https://en.wikipedia.org/wiki/Bryce\\_DeWitt](https://en.wikipedia.org/wiki/Bryce_DeWitt)>

O *teorema de Bell* é o legado mais importante do físico teórico **John Bell**, publicado em 1964, que estabelece uma distinção absoluta entre a *mecânica quântica* e a *mecânica clássica*, ou seja, não existe regime de variáveis ocultas locais que possam reproduzir todos os resultados da mecânica quântica.

Na realidade, o *teorema de Bell* consistia em uma *classe de desigualdades*, uma das quais foi demonstrada por **John Bell**, que no meado dos anos 60 examinou criticamente a proposta apresentada por **John von Neumann**, da não-existência de variáveis ocultas. **Bell** mostrou que a hipótese do *realismo local*, ou seja, que:

1. Uma partícula possui valores definitivos que não dependem do processo de observação e,
2. A velocidade de propagação dos efeitos físicos é finita e, não é compatível com a mecânica quântica.

O *Teorema de Bell* ofereceu uma forma de quantificar alguns conceitos associados com o paradoxo EPR e permitiu, por fim, os testes experimentais de **rede quântica** versus *realismo local*. Foi comprovado pela primeira vez em 1972 por **John Clauser**, de Berkeley.

O fenômeno do *entrelaçamento quântico* que está por trás da violação das *desigualdades de Bell* é um dos elementos da Física Quântica que não pode ser representado





Figura 71 – John Bell - Concluiu que nenhuma teoria de variáveis locais ocultas poderia ser válida no contexto da mecânica quântica.

Fonte: <[https://en.wikipedia.org/wiki/John\\_Bell](https://en.wikipedia.org/wiki/John_Bell)>

em qualquer outra visão clássica da Física.

Alguns defensores da ideia das *variáveis ocultas* preferem aceitar a opinião de que estes experimentos são controlados de fora por *variáveis ocultas locais*. Eles estão prontos para abrir mão da localidade, explicando a *violação da desigualdades de Bell* por meio de uma *teoria de variáveis ocultas não locais*, na qual as partículas trocam informação a respeito de seus estados. Esta é a base do interpretação de **Bell** da mecânica quântica.

**Bell** foi o primeiro a mostrar que a prova de **John von Neumann**, contra o determinismo da mecânica quântica possuía falhas e, que o trabalho de **David Bohm** contornava as objeções de **John von Neumann**. A falha na prova de **von Neumann's** foi primeiramente descoberta por **Grete Hermann** (1901-1984) em 1935, mas não tornou-se conhecida até ser redescoberta por **Bell**.

**Grete Hermann** foi uma filósofa e matemática alemã. Estudou matemática em Göttingen, onde recebeu seu Ph.D. em 1926. Sua tese de doutorado, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, publicada em *Mathematische Annalen* é o trabalho inicial para *álgebra computacional*. Este trabalho é o primeiro a estabelecer a existência de algoritmos (incluindo nível de complexidade) para muitos dos problemas básicos da álgebra abstrata, tais como agrupamentos *ideais* para *anéis polinomiais*. O *algoritmo de Hermann* para decomposição primária é ainda usado hoje. Como uma filósofa, **Grete Hermann** tinha um interesse particular pelos fundamentos da Física. Em 1935 ela descobriu uma falha na suposta prova de **John von Neumann**, de 1932, que uma teoria de variáveis ocultas da mecânica quântica era impossível. Este resultado passou despercebido pela comunidade científica até



Figura 72 – John von Neumann - A proposta da não-existência de variáveis ocultas

Fonte: <[https://en.wikipedia.org/wiki/John\\_von\\_Neumann](https://en.wikipedia.org/wiki/John_von_Neumann)>

que foi redescoberto, vinte anos mais tarde, por **John Stewart Bell**.

Em 1972 a primeira de muitas experiências que mostrariam a violação da *Desigualdade de Bell* foi realizada. Foi comprovado pela primeira vez em 1972 por **John Clauser** (1942-...), de Berkeley, um físico teórico e experimental estadunidense, conhecido por suas contribuições aos fundamentos da mecânica quântica.

Este fato mostrou que o destino de teorias envolvendo *variáveis locais ocultas* estava selado. O *teorema de Bell* podia ser considerado como uma prova de que uma teoria universal deve envolver mecânica quântica. **Bell** tornou-se um suporte para a interpretação de **David Bohm**, uma *teoria de variáveis ocultas não locais envolvendo sinais*, e começou a defender o seu trabalho contra aqueles que favoreciam o *indeterminismo da mecânica quântica* tais como a *Interpretação de Copenhague* e a *Interpretação de Muitos Mundos*.

Os resultados das experiências, mostrando que eles violavam suas desigualdades, não fizeram **John Bell** particularmente feliz: ele esperava que essas pudessem sempre ser satisfeitos na natureza, e que as experiências eventualmente negariam a mecânica quântica. Apesar de observar as violações, ele manteve alguma esperança que as experiências futuras deveriam mudar a situação. Não obstante, ele estava pronto para aceitar a validade da mecânica quântica ortodoxa. Seguidores do *realismo local e teoria quântica* continuam igualmente a procurar por soluções que expliquem as aparentes falhas da *realidade local* nos experimentos de teste de **Bell**.

Os resultados das experiências, mostrando que eles violavam suas desigualdades, não fizeram **John Bell** particularmente feliz: ele esperava que eles pudessem sempre ser satisfeitos na natureza, e que as experiências eventualmente negar a mecânica quântica. Apesar de observar as violações, ele manteve alguma esperança que as



Figura 73 – Grete Hermann - O trabalho precursor para a álgebra computacional.

Fonte: <[https://en.wikipedia.org/wiki/Grete\\_Hermann](https://en.wikipedia.org/wiki/Grete_Hermann)>

experiências futuras deveriam mudar a situação. Não obstante, ele estava pronto para aceitar a validade da mecânica quântica ortodoxa. Referindo-se aos teste dos experimentos de Bell, um comentário seu é frequentemente citado:

*"É difícil para eu acreditar que a mecânica quântica, funcionando muito bem para actuais parâmetros práticos, não obstante venham a falhar completamente com a melhoria da eficiência dos experimentos..."* (Ref 1, page 109) Bell (1987)

Algumas pessoas continuam a acreditar que a *mecânica quântica probabilística* deva estar errada. Seguidores do *realismo local* e *teoria quântica* continuam igualmente a procurar por soluções que expliquem as aparentes falhas da realidade local nos experimentos do teste de Bell.

Em vistas dos resultados experimentais oriundos, entre outros, de investigações quanto à desigualdade de **Bell**, a maioria dos físicos atuais concorda que o paradoxo EPR é decidido a favor de que a mecânica quântica está além dos limites da *Física Clássica* e da *Relatividade Restrita*; e não a favor de que teoria quântica seja uma teoria incompleta, falha ou mesmo incompatível com a descrição da natureza em sua essência mais profunda. Os dados experimentais até o momento decidem a favor da *compreensão ortodoxa do estado emaranhado* (a chamada *Interpretação de Copenhagen*). Um razoável esforço da comunidade de físicos tem sido despendido desde então no intuito de elaborar-se uma *teoria quanto-relativística* que possibilitasse uma

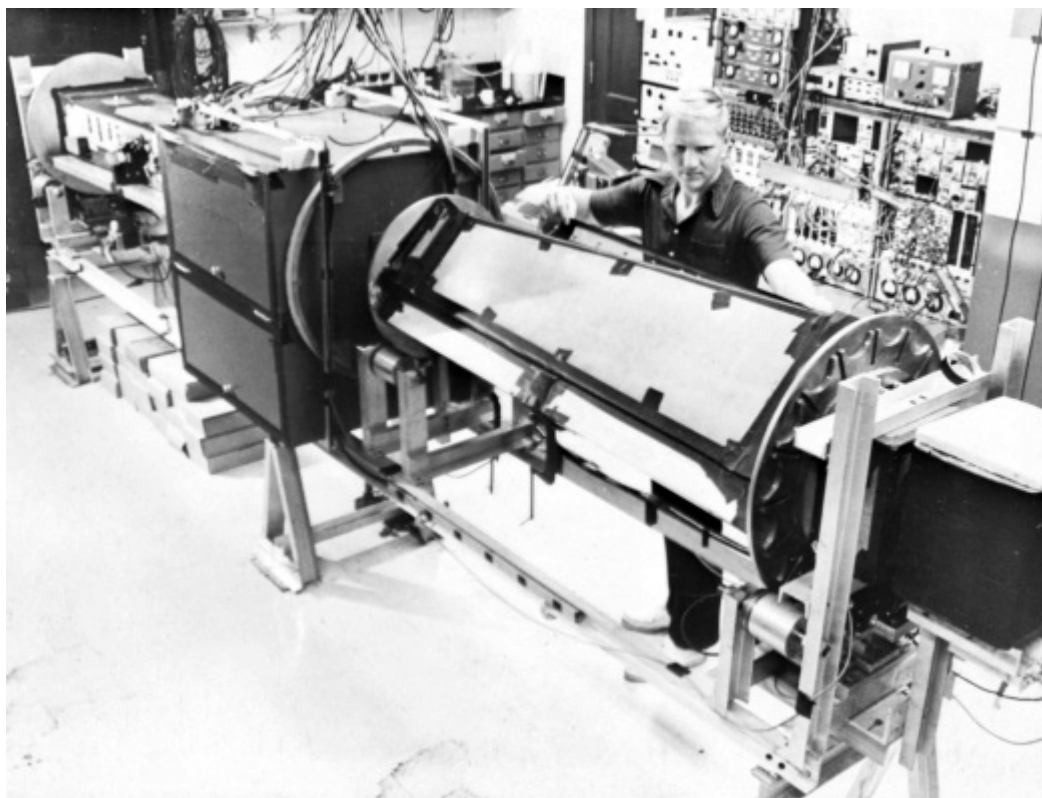


Figura 74 – John Clauser - A prova da violação das desigualdades de John Bell.

Fonte: <[https://en.wikipedia.org/wiki/John\\_Clauser](https://en.wikipedia.org/wiki/John_Clauser)>

descrição mais acurada da natureza, do que a fornecida pelas duas teorias, quando em suas formas independentes.

## 4.15 O primeiro round

**Samuel Johnson** (1709-1784) foi um escritor e pensador inglês conhecido por suas notáveis contribuições à língua inglesa como poeta, ensaísta, biógrafo, crítico literário e lexicógrafo. Ele foi *a person who records in detail the life of a usually famous contemporary*, mas **John Archibald Wheeler** (1911-2008), um físico teórico estadunidense, um dos últimos colaboradores de **Albert Einstein**, não ficou atrás. Ele tentou formular a concepção de **Einstein**, sobre uma *teoria do campo unificado* e introduziu a *Matriz S*, fundamental na Física de Partículas. (STEIN, 2008)

**John Wheeler** certamente merece este patamar - pois, possivelmente nenhum outro físico ou matemático será capaz de sintetizar os dilemas enfrentados pela ciência de modo tão sucinto. Um componente-chave da incompatibilidade entre a Física do grande (relatividade) e a Física do pequeno (mecânica quântica) é o modelo matemático usado para descrevê-la. No nível do muito pequeno, o vencedor incontestado - por enquanto - é a *visão discreta*, pois a hipótese de **Mark Planck** resultou em descrições discretas que se mostraram incredivelmente eficientes para prever os valores de todas as quantidades físicas relevantes do nível do muito pequeno.



Figura 75 – John Archibald Wheeler - Físico estadunidense, um dos últimos colaboradores de Einstein.

Fonte: <[https://pt.wikipedia.org/wiki/John\\_Archibald\\_Wheeler](https://pt.wikipedia.org/wiki/John_Archibald_Wheeler)>

## 4.16 A incerteza por princípio

A Física clássica é fundamentada pela descrição dos movimentos dos corpos introduzida por **Isaac Newton** (1643-1727) [Newton \(1999\)](#), e também pela descrição do comportamento dos campos e ondas eletromagnéticas compilada por **James Clerk Maxwell** (1831-1879).

As várias teorias, teoremas e experimentos construídos ao longo dos últimos séculos pelos sucessores e até mesmo antecessores de Newton e Maxwell demonstraram que as equações da mecânica e do eletromagnetismo descrevem com grande sucesso os fatos observados. No início do século passado, alguns experimentos ficavam inexplicados: por exemplo, pela teoria do eletromagnetismo, um elétron quando acelerado emite energia na forma de radiação eletromagnética e com isto, baseado no princípio da conservação da energia, diminui sua própria energia de movimento. Decorrente deste fato, um elétron submetido à ação de uma força centrípeta em um movimento ao redor do núcleo, deve perder sua energia e se precipitar no núcleo, o que não ocorre.

Outras contradições entre fatos reais/experimentais e previsões teóricas surgiram, entre eles um famoso problema, a catástrofe do ultravioleta de **Rayleigh** e **Jeans** ([BAGGOT, 2004](#)). O problema considera que um corpo negro teria uma energia infinita, a energia é função da temperatura e da frequência da radiação eletromagnética. Dada uma frequência, a energia obtida é uma integral em um intervalo contínuo e isto faz com que esta integral resulte em valor infinito quando calculada para frequências na região do ultravioleta. **Max Planck** resolveu este problema, ele propôs que a energia não assumia valores contínuos, e sim múltiplos de um valor mínimo:  $E = n.h$ , sendo a frequência,  $h$  uma constante (constante de Planck) e  $n$  valores inteiros, o valor mínimo possível:  $E = n.h$  é o *quanta* de energia. Com isto a energia total passou a ser uma soma discreta, e não mais uma integral (soma contínua), coerente com os resultados experimentais. Com a definição do *quanta* de energia, os valores de energia possíveis são, agora, "quânticos". Este foi o primeiro trabalho que deu

início à Física Quântica.

**Heisenberg** em seu trabalho sobre princípios da teoria quântica ([HEISENBERG, 1949](#)), trouxe uma compilação de vários experimentos que apresentava a ambiguidade entre a natureza corpuscular e ondulatória da matéria. Por exemplo, raios ao passarem por uma câmara de bolhas deixam um rastro compatível com a natureza de uma partícula, e é possível determinar massa e velocidade. Por outro lado, os raios ao atravessarem um filme fino de material cristalino formam uma figura de difração em um anteparo, compatível com a natureza de uma onda, e é possível medir sua frequência. Isto significa que um feixe de raios pode ser descrito tanto como uma frente de onda quanto como um conjunto de partículas.

O mesmo foi observado para os raios X, que como são radiações eletromagnéticas, possuem a natureza de onda. Quando um feixe deste raio atravessa um vapor supersaturado de água, é deixado um rastro tal qual um conjunto de partículas, também se observa o efeito de difração para o raio X. Decorrente da natureza dual partícula-onda, **Heisenberg** deduziu que o conhecimento da posição de uma partícula com a precisão  $x$ , e o conhecimento do momento (velocidade) da partícula com a precisão  $p$ , deve obedecer o limite:  $x\Delta p > h$ , sendo  $h$  a *constante de Planck*. Este resultado é conhecido como o **Princípio da Incerteza de Heisenberg**, e deriva diretamente da dualidade partícula-onda, não sendo possível conhecer simultaneamente a posição e velocidade de uma partícula, exceto dentro de um limite de incerteza, que é pequeno comparado ao valor da massa de corpos do nosso cotidiano, mas é expressivo em um mundo subatômico.

Enquanto realizava experiências para evidenciar a dualidade partícula-onda também para a luz que é uma forma de radiação eletro-magnética, **Eisntein** demonstrou através do *efeito foto-elétrico*, o que lhe valeu um prêmio Nobel, que a luz também pode ser interpretada na forma de partícula, chamada *fóton*. Com base nisso, propôs uma experiência na obtenção de figuras de difração a partir de fótons ([RAE, 1986-2004](#)). Nesta experiência emite-se luz com intensidade bem baixa, quase que um fóton por vez, de forma a passar por um anteparo com dois furos, observa-se que no resultado cada fóton imprime uma imagem que compõe ao longo do tempo, com a imagem de outros fótons, a figura da difração. Isto indica que a natureza *onda* do fóton permite que este, mesmo sendo uma única partícula, atravesse ao mesmo tempo ambos furos formando a figura de difração, e cada fóton acaba sendo impresso como um ponto, ou partícula, no anteparo. Se for colocado um tipo de detecção, logo na saída dos furos para identificar por qual furo o fóton passa, de fato, observa-se que cada foton passa por um único furo, no entanto perde-se a figura de difração. A medida da posição ou velocidade do fóton afeta seu estado.

O **princípio da incerteza** e o resultado de que uma medida afeta o estado de uma partícula nos limites quânticos, nos permitirá entender o modelo da computação quântica. ([STEIN, 2008](#))

## 4.17 Bibliografia e Fonte de Consulta

J. Bronowski - (*The Ascent of Man* (Boston: Little, Brown, 1973), p.336. Edição brasileira: *A Escalada do Homem* (São Paulo: Liv. Martins Fontes; Brasília: Ed.Universidade de Brasília, (1983).

Baggot, J. *Beyond Measure - Modern Physics, Pylosophy and the Meaning of Quantum Theory*. Oxford University Press, 2004.

Heisenberg, W. *The Physical Principles of the Quantum Theory* - Translated by Eckart C. and Hoyt F. C. Dover Publications, 1949.

Newton, I. *The Principia - Mathematical Principles of Natural Philosophy* - A new translation by Cohen, I. B. and Whitman, A. University of California Press, 1999.

Rae, A. *Quantum Physics - Illusion or Reality ?*, Cambridge University Press.

Masud Chaichian; Andrei Pavlovich Demichev . *Introduction to Path Integrals in Physics, Volume 1: Stochastic Process & Quantum Mechanics*. [S.l.]: Taylor & Francis. p. 1 ff. ISBN 0-7503-0801-X., 2001.

Dirac, Paul A. M., *The Lagrangian in Quantum Mechanics*. *Physikalische Zeitschrift der Sowjetunion*. 3: 64-72. 1933.

Feynman, Richard P. (Richard Phillips); Hibbs, Albert R.; Styer, Daniel F. . *Quantum Mechanics and Path Integrals*. Mineola, N.Y.: Dover Publications. pp. 29-31. ISBN 0-486-47722-3., 2010.

P. A. M. Dirac. *On the quantum theory of the electron* (PDF).

Em <<https://www.rpi.edu/dept/phys/Courses/PHYS6520/DiracElectron.pdf>>

*Antimatéria*, site do Departamento de Física Nuclear do Instituto de Física da Universidade de São Paulo. Em <<https://pt.wikipedia.org/wiki/Antimatéria>>

*Fóton* - <<https://www.infoescola.com/fisica/foton/>>

## 4.18 Referências e Leitura Recomendada

Experimento da dupla fenda de Young, realizado com elétrons - <<http://www.if.ufrgs.br/historia/young.html>>, acessado em 16/10/2017.

Gillispie, Charles Coulston (1997) *Pierre Simon Laplace 1749-1827: A Life in Exact Science*, Princeton: Princeton University Press, ISBN 0-691-01185-0.

Hahn, Roger (2005) *Pierre Simon Laplace 1749-1827: A Determined Scientist*, Cambridge, MA: Harvard University Press, ISBN 0-674-01892-3.

Leite Vieira, Cásio. - "Há 50 anos, o físico norte-irlandês John Bell (1928-90) chegou a um resultado que demonstra a natureza "fantasmagórica" da realidade no mundo atômico e subatômico.", Site Folha de S.Paulo. Consultado em 10 de dezembro de 2017, <<http://www1.folha.uol.com.br/ilustrissima/2014/12/1566019-particulas-telepaticas.shtml>>.

Pearle, P, *Hidden-Variable Example Based upon Data Rejection*, *Physical Review D*, 2, 1418-25 (1970).

Aczel, Amir D, Entanglement: The greatest mystery in physics, Four Walls Eight Windows, New York, 2001.





# Os Experimentos da Dupla-Fenda

Partículas e ondas se comportam de maneiras diferentes quando passam através de fendas. As ondas são perturbações que se propagam no espaço ou em meios materiais transportando energia.

## 5.1 Um experiência com projéteis

Para mostrar que os **objetos microscópicos não se comportam nem como ondas nem como partículas**, escolhemos um experimento onde este comportamento se manifesta de forma marcante: a experiência de interferência por uma fenda dupla. Tornaremos a tratar deste caso (ondas) em breve, mas, inicialmente, iremos descrever o comportamento de projéteis (balas de canhão ou bolinhas de gude, por exemplo) ao passar por uma fenda dupla. Em seguida, iremos analisar o comportamento das ondas e, finalmente, o comportamento de objetos microscópicos, como os elétrons. O aparato experimental está esquematizado na Figura 76 (a).

Há uma metralhadora que dispara projéteis, um de cada vez, em direções aleatórias. Em frente à metralhadora, há uma parede que impede a passagem dos projéteis, exceto por dois pequenos buracos. Mais adiante, há um anteparo, onde os projéteis que conseguem passar pelos buracos se alojam, e sua chegada é verificada por um detetor deslocável. Este detetor pode ser uma caixa com areia, por exemplo, onde os projéteis se depositam. Depois, podemos contar quantos projéteis chegaram em cada posição da parede em um certo intervalo de tempo. A posição ao longo da parede é descrita por uma coordenada  $x$ , medida a partir do centro.

Nossa primeira observação parece um pouco óbvia, dada nossa grande intuição com partículas clássicas: cada projétil chega intacto ao detetor, como se fossem "pacotes" idênticos, um de cada vez. É claro, estamos supondo que são projéteis indestrutíveis... Não se observa a chegada de "meio projétil" ou a chegada de dois projéteis simultaneamente em lugares diferentes. Projéteis sempre chegam em pacotes idênticos. Em seguida, usando esse aparato simples, podemos tentar responder à seguinte pergunta: "Qual a probabilidade de um projétil acertar a posição  $x$ ?" Naturalmente, temos de falar em probabilidades, pois é impossível saber com certeza absoluta a trajetória de cada partícula, já que elas são lançadas em direções aleatórias e podem ricochetear de forma imprevisível nas bordas dos buracos. Mas

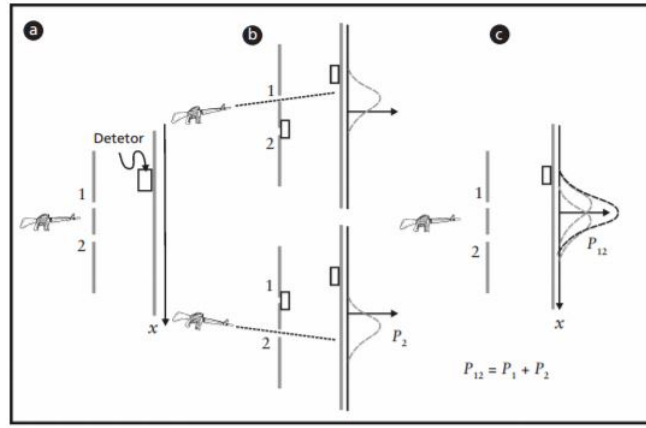


Figura 76 – Experimento da Dupla Fenda com Projéteis - (a) Esquema do experimento de fenda dupla com projéteis. (b) Situação experimental e distribuições de probabilidades obtidas quando uma das fendas é fechada. (c) Situação experimental e distribuição de probabilidade obtida quando as duas fendas estão abertas.

Fonte: <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula01.pdf>>

a probabilidade pode ser facilmente medida, tomando-se a fração de projéteis que chegam a uma certa posição em relação ao número total de projéteis que acertam todo o anteparo, no mesmo intervalo de tempo. Se fizermos a medida, obteremos a distribuição de probabilidades  $P_{12}$  mostrada na Figura 76 (c), que tem este nome porque os projéteis podem passar tanto pelo buraco 1, como pelo buraco 2. A curva  $P_{12}$  tem um máximo em torno de  $x = 0$  e decai para valores muito pequenos se tomamos valores de  $x$  muito distantes da origem.

Mas, por que o valor máximo de  $P_{12}$  fica em torno de  $x = 0$ ? De fato, isto acontece apenas se a distância entre os buracos for suficientemente pequena, mas é com esta situação que queremos lidar. Podemos entender isto se fizermos novamente o experimento, mas, desta vez, fechando um dos buracos, como mostra a Figura 76 (b). Se fechamos o buraco 2, medimos a distribuição de probabilidades  $P_1$  mostrada no painel superior. E se fechamos o buraco 1, medimos a distribuição  $P_2$  mostrada do painel inferior. Como esperado, a distribuição  $P_1$  tem seu valor máximo na posição  $x$  na parede que está ao longo da reta tracejada que vai da metralhadora ao buraco 1. E a distribuição  $P_2$  se comporta de forma análoga. A distribuição conjunta  $P_{12}$  é simplesmente a soma das distribuições parciais:

$$P_{12} = P_1 + P_2 \quad (5.1)$$

Ou seja, o efeito obtido quando temos os dois buracos abertos é a soma dos efeitos de cada buraco individualmente. Isto quer dizer que projéteis não sofrem interferência, como veremos a seguir que ocorrem com ondas. Isto resume nosso entendimento sobre projéteis incidindo em uma fenda dupla: primeiro, eles chegam em pacotes idênticos; segundo, não apresentam interferência.

Veja este exemplo. Uma metralhadora despeja balas em uma fenda dupla, como mostrado na Figura 76. As balas passam pelo buraco 1. Elas, então, se depositam no

anteparo, de acordo com uma distribuição de probabilidades que pode ser aproximada por uma gaussiana com largura, e máximo em  $x = d$ , ou seja,  $P_1(x) = A \cdot e^{-(x-d)^2/2\sigma^2}$ , onde  $A$  é um fator de normalização. Já as balas que passam pelo buraco 2 se depositam em torno de  $x = -d$  de forma análoga:  $P_2(x) = A \cdot e^{-(x+d)^2/2\sigma^2}$ . Se a largura  $\sigma$  for muito maior que  $d$ , a distribuição resultante ( $P_{12} = P_1 + P_2$ ) terá um único pico, como na Figura 76 (c). Porém, se  $\sigma$  for muito menor que  $d$ , a distribuição resultante terá dois picos. O que pode ser encontrado neste experimento é, em função de  $d$ , o valor de  $\sigma$  que separa estes dois regimes.

Graficamente, é muito claro observar, se uma curva tem um pico ou dois picos. A dificuldade deste problema está em expressar matematicamente estas situações. Bem, sabemos que uma função que apresenta um máximo local tem derivada nula neste ponto e derivada segunda negativa. Já se a função tiver um mínimo local, ela terá derivada nula e derivada segunda positiva. Faça agora um esboço da distribuição  $P_{12}$  nas duas situações: com um pico e com dois picos. Quais as diferenças essenciais entre os dois gráficos que você fez? Uma delas é óbvia: uma distribuição tem um pico e a outra tem dois. Mas repare também no comportamento de  $P_{12}$  na posição  $x = 0$ . Note que  $P_{12}$  será máxima neste ponto se tiver um pico (na verdade, o pico ocorre precisamente em  $x = 0$ ) ou será mínima se tiver dois picos. Como dissemos, o que distingue matematicamente estas duas situações é o sinal da derivada segunda. Assim, o valor limítrofe de  $d$ , que separa estes dois regimes, pode ser encontrado impondo a condição de derivada nula, ou seja, nem positiva nem negativa. Portanto, impondo a condição:

$$\frac{d^2}{dx^2} P_{12} \Big|_{x=0} = 0$$

chegaremos na resposta, depois de algum algebrismo.

## 5.2 Uma experiência com ondas de água

Se imaginarmos ondas batendo num litoral (**ondas de água**), bloqueadas por um cais de pedra com uma abertura estreita, as ondas se espalham para fora em círculos concêntricos em volta da abertura. Se houver duas aberturas razoavelmente próximas uma da outra, as ondas se espalham para fora em círculos concêntricos em volta de cada abertura. Mas as ondas de cada abertura interferem com as ondas da outra abertura. Onde os pontos mais altos das ondas de um conjunto de ondas encontramos mais mais altos de outro conjunto de ondas, esses pontos mais altos ficam reforçados. Quando os pontos mais baixos de um conjunto de ondas encontram os pontos mais baixo de outro conjunto de ondas, elas tendem à neutralização mútua, diminuindo a amplitude dos pontos mais baixos, onde esses pontos mais baixos se encontram.

O comportamento das partículas ao encontrarem uma coleção de aberturas estreitas, é diferente. Se duas peças de papelão estão alinhadas em paralelo uma atrás da outra, e uma única fenda estreita é cortada numa delas, quando um spray de tinta é dirigido à fenda, uma única mancha de tinta aparecerá na peça mais distante de papelão, diretamente atrás da fenda. As margens da mancha não são claramente definidas. As partículas de tinta se espalharam a partir do centro, mas diminuem em densidade à medida que se afastam do centro. Contendo-se duas fendas paralelas próximas, na peça com a primeira fenda e direcione o spray de tinta a ambas as

fendas. Manchas similares aparecerão na peça de papelão mais distante, diretamente atrás das fendas.

Vamos ver agora o que acontece quando usamos o mesmo aparato experimental para estudar o comportamento de **ondas de água** (e não mais de projéteis). O esquema da experiência está mostrado na Figura 77. No lugar do canhão, temos agora um dispositivo gerador de ondas circulares, uma fonte de ondas. Pode ser, por exemplo, um pequeno objeto que oscila para cima e para baixo na superfície da água. Temos ainda a parede com dois buracos e, mais adiante, um anteparo absorvedor de ondas, construído de modo que as ondas não sejam refletidas ao incidirem sobre ele (uma praia em miniatura, por exemplo). No anteparo absorvedor, coloca-se um pequeno detetor da intensidade das ondas, do qual podemos variar a posição  $x$ . Este detetor pode ser uma pequena bóia que oscila para cima e para baixo, ao sabor das ondas que chegam até ela: **a intensidade da onda não é exatamente a amplitude da oscilação deste objeto, mas sim proporcional ao quadrado da amplitude!**

O que observamos quando fazemos o experimento? Em primeiro lugar, observa-se que a *onda* que chega ao detetor pode ter qualquer intensidade. Ou seja, a bóia pode ser mover com qualquer amplitude, ainda que seja muito pequena. Este resultado é bastante diferente do que observamos com *projéteis*: partículas "chegam" ou "não chegam" em pacotes iguais, ou seja, com intensidades "discretas" ou "quantizadas". Já as *ondas* chegam com qualquer intensidade, ou seja, a intensidade varia de forma "contínua".

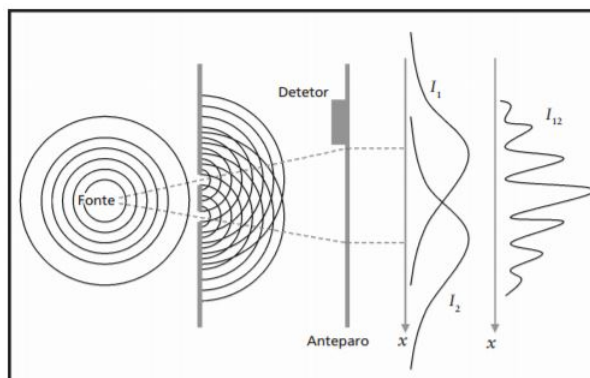


Figura 77 – Esquema do experimento de fenda dupla com ondas. As intensidades  $I_1$  e  $I_2$  correspondem às situações onde apenas os buracos 1 ou 2 estão abertos, respectivamente. Já a intensidade  $I_{12}$  corresponde à situação em que os dois buracos estão abertos simultaneamente.

Fonte: <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula01.pdf>>

Quando medimos a intensidade da onda  $I_{12}$  em função da posição  $x$  do detetor, obtemos o gráfico mostrado na Figura 77. Note que a intensidade oscila fortemente com a posição, passando por valores máximos (picos) e mínimos (vales). Este gráfico nos é familiar dos nossos estudos em física ondulatória e ótica: trata-se do conhecido padrão de interferência por uma fenda dupla. Conceitualmente, ele pode ser entendido a partir da ideia de que os buracos atuam como geradores de novas ondas circulares, que interferem construtiva ou destrutivamente. Se tamparmos um dos buracos, a interferência desaparece. A curva  $I_1$  da referida figura corresponde à situação em que apenas o buraco 1 é deixado aberto e, para a curva  $I_2$ , apenas o buraco 2 é

aberto. Note que estas curvas não têm as oscilações fortes da curva  $I_{12}$ , de modo que, claramente, notamos que  $I_{12} \neq I_1 + I_2$ .

Analisamos o experimento de fenda dupla realizado de duas formas distintas: uma com projéteis e a outra com ondas. Observamos que projéteis chegam ao detetor em pacotes idênticos e não apresentam interferência. Em contraste com este comportamento, as ondas podem ser detetadas com qualquer intensidade e apresentam interferência. Esses comportamentos são característicos das partículas e das ondas clássicas. Será interessante compará-los com o comportamento de partículas quânticas, o que faremos na próxima aula.

### 5.3 Uma experiência com ondas de luz

A experiência da dupla-fenda consiste em deixar que a luz visível se difracte através de duas fendas, produzindo bandas. As bandas formadas, ou padrões de interferência, mostram regiões claras e escuras que correspondem aos locais onde as ondas luminosas interferiram entre si construtivamente e destrutivamente. **Young** contruiu um experimento que se aproveitava dessa diferença. Ele cortou duas fendas paralelas em uma peça de papelão e projetou uma luz por essas fendas, sobre um fundo escurecido. Ele observou bandas brilhantes de luz alternadas, intercaladas com regiões totalmente escuras. Essa é a forma clássica de interferência de onda. As bandas brilhantes ocorriam onde os pontos altos da luz coincidiam, enquanto as bandas escuras, onde os pontos baixos de uma onda de luz eram canceladas pelos pontos baixos da outra onda de luz. Ver a Figura 79



Figura 78 – Thomas Young - Físico, a experiência da dupla fenda com ondas de luz.

Fonte: <[https://pt.wikipedia.org/wiki/Thomas\\_Young](https://pt.wikipedia.org/wiki/Thomas_Young)>

### 5.4 Uma experiência com ondas de um feixe eletrônico

No caso da realização da experiência da dupla fenda com um feixe eletrônico, imaginemos uma tela opaca aos elétrons, e nela fazemos duas pequenas fendas. Observando o passar do feixe de elétrons por uma destas fendas, com a outra fechada, obtemos numa tela plana colocada atrás da fenda uma certa figura de distribuição das intensidades; da mesma maneira obtemos outra figura semelhante à primeira

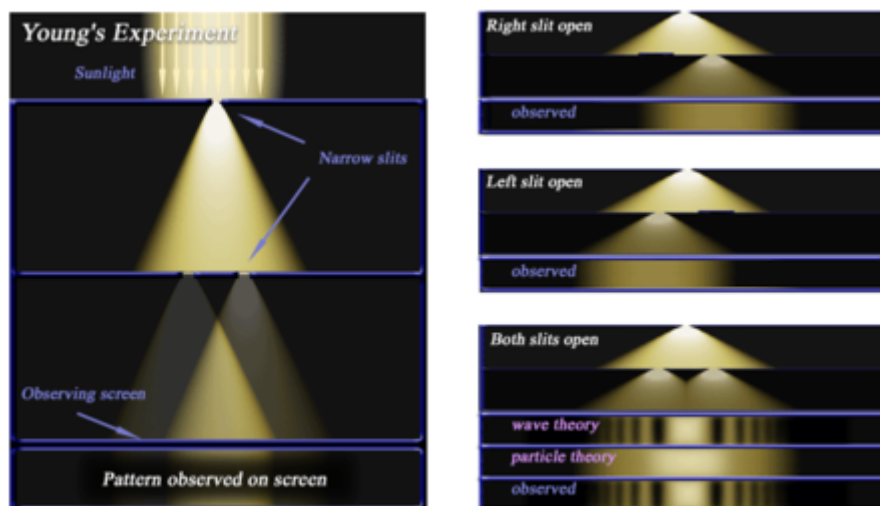


Figura 79 – Experimento da Dupla Fenda - a luz visível se difracta através de duas fendas.

Fonte: <[https://pt.wikipedia.org/wiki/Experiencia\\_da\\_dupla\\_fenda](https://pt.wikipedia.org/wiki/Experiencia_da_dupla_fenda)>

abrindo a segunda fenda e fechando a primeira.

Mas, observando a imagem que se faz dos elétrons passando pelas duas fendas abertas ao mesmo tempo, baseando-nos nas ideias ordinárias, deveríamos observar uma figura consistente onde houvesse a simples superposição dos feixes complementares. Ou seja, a soma natural dos dois feixes que se projetariam na tela, uma vez que cada elétron partícula material movendo-se em sua trajetória fixa e bem delineada passa pela fenda sem exercer influência alguma sobre os outros elétrons que passam pela outra fenda.

O fenômeno da difração eletrônica mostra que na realidade obtemos uma figura de difração que ocorre em virtude da interferência e não se reduz de modo algum à simples soma das figuras produzidas por cada uma das fendas separadamente. Isso pode ser explicado simplesmente se for observado que em pontos mais distantes do lado direito da figura as ondas provenientes da fenda direita chegam primeiro do que as ondas da fenda esquerda, ocasionando um atraso no comprimento de onda original (que estavam exatamente sobrepostos no ponto central entre as fendas) gerando uma destruição ou construção da luz.

Diferença de Fase - Está claro que é impossível fazer coincidir este resultado com a ideia de movimento dos elétrons por uma trajetória. Pois a interferência que aparece é devido à somatória ora construtiva, ora destrutiva que indica diferenças de fase, isto é, neste caso, se há diferença de fase, então temos a natureza ondulatória dos elétrons que devem ser encarados, em analogia, como onda eletromagnética que se propaga pelo espaço e não como partícula material com movimento balístico, isto é disparada.

**Mecânica Quântica x Mecânica Clássica** - A experiência da dupla fenda prova inequivocamente a chamada *mecânica quântica* ou ondulatória, que deve basear-se em noções essencialmente diferentes da mecânica clássica. Pois na quântica não

existe o conceito de trajetória da partícula. Esta circunstância constitui o conteúdo do chamado *princípio da incerteza*, que é um dos fundamentais da mecânica quântica e foi proposto em 1927 por **Werner Heisenberg**.

## 5.5 Uma experiência com elétrons

- Vamos ver agora o que acontece quando realizamos o mesmo experimento de fenda dupla, mas agora com elétrons. Para isso, foi usado um canhão de elétrons. Este pode ser um fio metálico de tungstênio (como o filamento de uma lâmpada) que, quando aquecido, emite elétrons. Como nos dois experimentos descritos na aula anterior, os elétrons incidem sobre uma parede que tem dois buracos e atingem um anteparo no qual há um detetor deslocável. Um detetor para elétrons pode ser um *Contador Geiger* ou um multiplicador de elétrons que, conectado a um alto-falante, produz um ruído toda vez que for atingido por um elétron. A primeira coisa que pode ser notado é que a chegada dos elétrons no detetor produz sons de "cliques" bem definidos, vindos do alto-falante. Se interpretamos um som de "clique" como sendo a chegada de um elétron no detetor, quase todas as observações levam a crer que os elétrons se comportam como projéteis:

- a. Todos os "cliques" são idênticos: não existem "meios-cliques", por exemplo. Portanto, os elétrons chegam em pacotes idênticos.
- b. Os "cliques" acontecem de forma aleatória, ou seja, ouve-se algo como: clique.... clique..... clique-clique.. clique..... clique-clique-clique..... ..... clique. A análise desse padrão parece indicar que o instante de chegada de cada elétron é imprevisível.
- c. Nunca escutamos dois "cliques" simultaneamente, mesmo que coloquemos vários detetores cobrindo totalmente o anteparo. Isso quer dizer que os elétrons chegam um de cada vez.
- d. Se aumentarmos a temperatura do fio, teremos mais elétrons chegando ao detetor por unidade de tempo. Assim como fizemos com projéteis, podemos associar a taxa média de chegada dos elétrons à probabilidade de chegada, para cada posição  $x$  no anteparo.

As probabilidades  $P_1$  e  $P_2$  correspondem, respectivamente, às situações nas quais apenas os buracos 1 ou 2 estão abertos. Já a probabilidade  $P_{12}$  corresponde à situação em que os dois buracos estão abertos simultaneamente.

O que acontece então quando computamos esta probabilidade? Bem, todos os resultados descritos anteriormente parecem ser consistentes com o fato de o elétron ser um projétil, como uma pequeníssima bolinha de gude. Portanto, nada mais razoável do que esperar que observemos a mesma curva descrita na Figura 76. Aliás, toda a nossa intuição clássica nos leva a pensar no elétron como uma "bolinha". Pois bem, este é o momento crucial em que nossa intuição falha. A probabilidade  $P_{12}$  que medimos para o elétron está mostrada na Figura 80. Note que ela tem oscilações que não existiam no caso dos projéteis. De fato, elas lembram muito as oscilações que observamos no caso das ondas e que interpretamos como interferência.



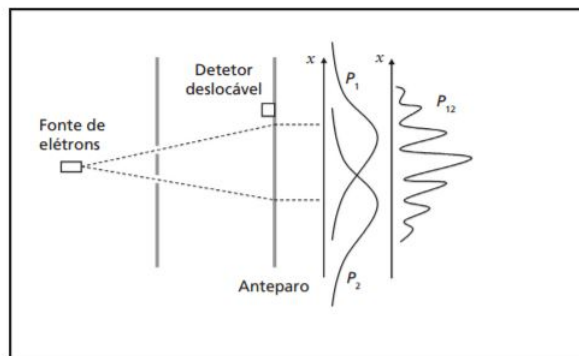


Figura 80 – Esquema do experimento de fenda dupla com elétrons.

Fonte: <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula02.pdf>>

### 5.5.1 Interferência de ondas de elétrons

Mas como pode surgir um padrão de interferência de projéteis? Vimos, no caso das ondas, que há uma interferência entre as ondas que passam pelo buraco 1 e as que passam pelo buraco 2. As ondas passam ao mesmo tempo pelos dois buracos. Poderiam os elétrons que passam pelo buraco 1 estar interferindo de alguma forma com os que passam pelo buraco 2? Sabemos que os elétrons são partículas carregadas negativamente e que, portanto, devem interagir entre si de acordo com a *Lei de Coulomb*. A Lei de Coulomb é uma lei da física que descreve a interação eletrostática entre partículas eletricamente carregadas. Foi formulada e publicada pela primeira vez em 1783 pelo físico francês **Charles Augustin de Coulomb** e foi essencial para o desenvolvimento do estudo da Eletricidade.

Poderia o padrão complicado de interferência surgir por meio da interação coulombiana ou, em outras palavras, a partir de um intrincado mecanismo de colisões entre os elétrons? Podemos testar experimentalmente esta hipótese. Já dissemos que os elétrons chegam um de cada vez no anteparo. Mas talvez eles estejam sendo emitidos com uma taxa muito alta, de modo que possamos ter vários elétrons "em vô" ao mesmo tempo e, portanto, interferindo uns nas trajetórias dos outros. Mas se reduzirmos bastante a temperatura do filamento, podemos diminuir cada vez mais a taxa de emissão de elétrons, até o limite em que tivermos certeza de que há apenas um elétron viajando de cada vez desde o emissor até o anteparo. Dessa forma, não há como ocorrer uma interação entre eles. Se fizermos o experimento, a taxa de detecção dos elétrons no anteparo realmente diminui bastante. Os "cliques" se tornam cada vez mais espaçados.

Mas, depois de deixarmos o experimento funcionando por um longo tempo, vai se formando, lentamente, o mesmo padrão de interferência que observamos anteriormente. Nada muda. Parece incrível, mas os elétrons passam um de cada vez pelos buracos e, ainda assim, interferem! É como se o elétron "interferisse com ele mesmo"!

Dizer que um elétron interfere com ele mesmo parece ser uma contradição. Afinal, a própria palavra "interferência" sugere a atuação de dois ou mais objetos no processo. Quem primeiro propôs esta expressão, propositalmente contraditória, para enfatizar a natureza não-intuitiva da interferência quântica, foi o físico inglês **Paul Dirac**. Na ocasião, ele se referia à experiência da fenda dupla realizada com fótons e

as partículas de luz que já foram mencionadas. Mas a mesma ideia vale para elétrons também.

Na sua edição de setembro de 2002, a revista *Physics World* elegeu o experimento de fenda dupla com elétrons como o mais belo da história da Física! Veja este artigo em <http://physicsweb.org/articles/world/15/9/1>.

## 5.6 Experimento da Dupla-Fenda Virtual

Há vários sites na Internet nos quais podemos explorar o experimento de fenda dupla de forma "virtual". Aprender a interagir com um experimento virtual, será muito útil para entender o fenômeno que estamos descrevendo.

O leitor poderá ver uma montagem do experimento de fenda dupla, por exemplo, como a reproduzida na Figura 81. Esta montagem consiste em uma fonte de partículas, uma fenda dupla, uma lâmpada e um anteparo.

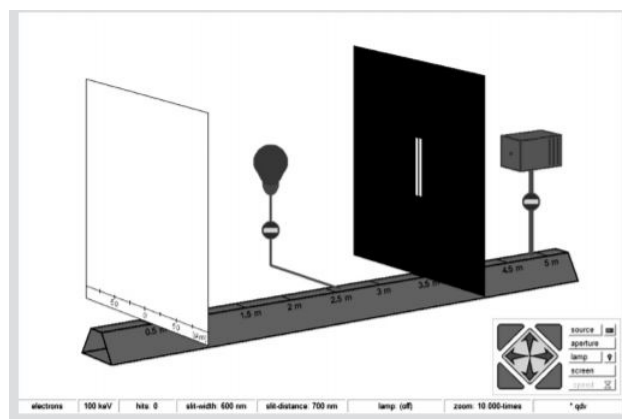


Figura 81 – Montagem experimental e painel de controle do experimento virtual de interferência por uma fenda dupla.

Fonte: <https://www.fing.edu.uy/if/cursos/fismod/cederj/aula02.pdf>

### 5.6.1 A experiência com elétrons

Deve ser observado que os elétrons colidem um de cada vez com o anteparo. Mas, gradualmente, surgirá na tela o padrão de interferências!

Ora, mas se os elétrons são pacotes idênticos e indivisíveis, poderíamos dizer que, diferentemente das ondas, eles passam ou por um buraco ou pelo outro, e não pelos dois ao mesmo tempo ?

Uma hipótese que pode ser testada:

*Hipótese - Cada elétron passa ou pelo buraco 1 ou pelo buraco 2. Pela nossa intuição com partículas clássicas, nada parece mais certo do que isso. Supondo que isto seja correto, todos os elétrons que atingem o anteparo se dividem em dois grupos: aqueles que passaram pelo buraco 1 e aqueles que passaram pelo buraco 2. Se isto for verdade, a curva  $P_{12}$  deve ser obtida pela soma de duas curvas:  $P_1$ , a distribuição de*

*probabilidades computada, usando apenas os elétrons que passaram pelo buraco 1, e  $P_2$ , usando apenas os elétrons que passaram pelo buraco 2. Será que podemos fazer este experimento?*

Fazendo-se o experimento, o resultado está reproduzido esquematicamente na Figura 81. O resultado experimental mostrará que  $P_{12} = P_1 + P_2$ .

Tudo parecerá muito misterioso. Elétrons chegam em "pacotes" e, ainda assim, exibem interferência típica das ondas. Este é um dos mistérios fundamentais da mecânica quântica: a *dualidade onda-partícula* no contexto do fóton. Como o físico americano **Richard Feynman** sugeriu -

*Vamos deixar de lado as tentativas de entender esse mistério. Tenha certeza de que muitos físicos famosos dedicaram boa parte de suas vidas tentando fazê-lo, sem sucesso. Vamos apenas aceitá-lo e explorá-lo um pouco mais. Ainda vamos descobrir coisas muito interessantes em consequência dele!*

A experiência de interferência de elétrons por uma fenda dupla foi realizada pela primeira vez por **Claus Jönsson** (1930-). Ele é um físico alemão que realizou em 1961, pela primeira vez, a versão do experimento da dupla fenda usando elétrons.



Figura 82 – Claus Jönsson - Em 1961, a primeira experiência de interferência de elétrons por fenda dupla.

Fonte: <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula02.pdf>>

Mais recentemente, em 1991, **Carnal** e **Mlynek** realizaram a mesma experiência com átomos em vez de elétrons. Sim, átomos, que são milhares de vezes mais pesados que os elétrons, e ainda assim são partículas quânticas. Em 1999, **Markus Arndt** (1965-), professor of *Quantum Nanophysics*, na *Faculty of Physics, University of Vienna* e outros colaboradores, viram a interferência de fenda dupla com moléculas de carbono C60, também chamadas de *buckyballs*. Estas moléculas, mostradas na Figura 83, contêm 60 átomos de carbono, dispostos como se formassem uma bola

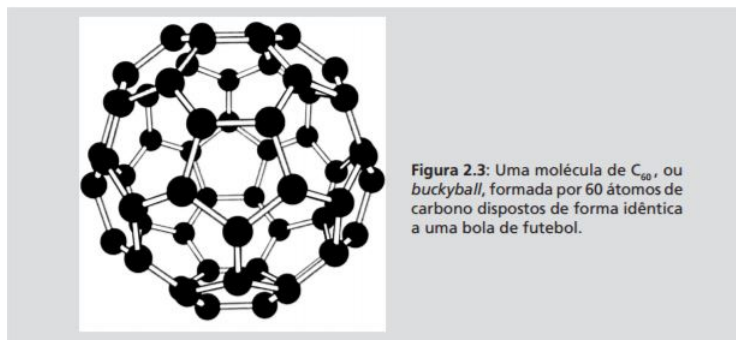


Figura 83 – Molécula de carbono 60 - A interferência de fenda dupla com moléculas de  $C_{60}$ .

Fonte: <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula02.pdf>>

de futebol. São centenas de milhares de vezes mais pesadas que um elétron. **Então, qual o limite que separa o mundo clássico do mundo quântico?**



Figura 84 – Markus Arndt - Em 1999, o físico que verificou a interferência de fenda dupla com moléculas de carbono  $C_{60}$ .

Fonte: <[https://de.wikipedia.org/wiki/Markus\\_Arndt](https://de.wikipedia.org/wiki/Markus_Arndt)>

Se  $P_{12} = P_1 + P_2$ , haverá alguma outra maneira de obtermos  $P_{12}$  a partir de  $P_1$  e  $P_2$ ? Surpreendentemente, a resposta é bastante simples. Basta usarmos a matemática das ondas. Note que a curva  $P_{12}$  é muito parecida com a curva de intensidades  $I_{12}$  que obtivemos na Aula 1 para as ondas. Como no caso das ondas, a intensidade não é a quantidade fundamental, mas sim a função de onda. Lembre-se: para ondas na superfície da água, a *função de onda* mais conveniente era a da altura do nível da água, que é considerada como uma variável complexa, para facilitar a matemática.

O físico francês **Pierre de Broglie** foi o primeiro a associar uma onda ao elétron. Na ocasião, essas ondas eram chamadas de "ondas de matéria". Segundo de

**Broglie**, um elétron (ou qualquer partícula microscópica) que se desloca com momento linear  $p$  tem associada a si uma onda com comprimento de onda  $\lambda$  tal que:  $\lambda = h/p$  (2.1), onde  $h = 6,63 \times 10^{-34}$  J.s é a constante de **Planck**. Vamos supor que o elétron é descrito por uma função de onda complexa  $\psi$ . Cada situação corresponde a uma função de onda diferente. Na Figura 81, se apenas o buraco 1 estiver aberto, teremos a função de onda  $\psi_1$ ; se apenas o buraco 2 estiver aberto, teremos a função de onda  $\psi_2$ ; e se ambos os buracos, 1 e 2, estiverem abertos, teremos a função de onda  $\psi_{12}$ . Em analogia com as ondas, temos que  $\psi_{12} = \psi_1 + \psi_2$ . A partir daí, como podemos obter as probabilidades relativas a  $\psi_1$  e  $\psi_2$ ? Podemos lembrar do caso das ondas, onde a intensidade era proporcional ao quadrado da amplitude da onda, pois algo análogo ocorre com o elétron, sendo que agora *a probabilidade é proporcional ao módulo quadrado da função de onda*. Como fizemos com as ondas na aula anterior, ignoramos, por enquanto, o coeficiente de proporcionalidade e escrevemos:

$$P_1 = |\psi_1|^2 \quad P_2 = |\psi_2|^2 \quad P_{12} = |\psi_1 + \psi_2|^2$$

Diz-se que a *função de onda de uma partícula quântica é uma amplitude de probabilidade*.

Lembre-se: para calcular o módulo ao quadrado de um número complexo, multiplica-se o número pelo seu complexo conjugado, ou seja,  $|\psi|^2 = \psi\psi^*$ . Note que  $|\psi|^2$  deve ser um número real e positivo. Afinal, toda probabilidade que se preza deve ser real e positiva.

Como se vê, a matemática das ondas nos explica naturalmente o resultado encontrado no experimento, pois dela surge naturalmente o fenômeno de *interferência entre ondas*. Mas então, se a soma dos efeitos de cada uma das ondas oriundas das fendas é diferente do efeito conjunto das duas fendas abertas, a Hipótese A está incorreta! Não é verdade que os elétrons passam por uma fenda ou pela outra fenda. Mas como pode ser isto, se eles chegam em pacotes? Será que eles fazem algo complicado, como se dividir em dois, passar pelas fendas e depois se juntar novamente em um só? Somos tentados a imaginar qualquer coisa, por mais absurda que seja, para salvar os conceitos clássicos de *partícula e trajetória*, bastante consolidados em nossa intuição física. Esta nos parece tão afrontada que não resistimos: temos de fazer um outro experimento para testar a Hipótese A. Será que não é possível observar os elétrons e ver por onde eles passam?

Partículas microscópicas, como elétrons, têm um comportamento peculiar ao passar por uma fenda dupla. Este comportamento é diferente tanto de projéteis como de ondas. Ele tem características de ambos, o que designamos como dualidade onda-partícula. É necessário aprender também a usar a matemática das ondas para calcular as probabilidades de encontrar o elétron em determinadas posições do espaço.

## 5.7 Polarização de Fótons

Como em (RIEFFEL; POLAK, 2000), vamos exemplificar um experimento simples para nos familiarizarmos com alguns fenômenos quânticos e exemplificar **observações** de fótons e **medições** realizadas por filtros de polarizações.

Os fótons são as únicas partículas que podemos **observar** diretamente. A seguinte

experiência simples pode ser executada com o mínimo de equipamento: uma fonte de luz forte, como um apontador laser, e três polaróides (*filtros de polarização*) que podem ser conseguidos em qualquer loja de suprimentos de câmeras. O experimento demonstra alguns dos princípios da mecânica quântica através de fótons e sua polarização (CARDONHA; SILVA; FERNANDES, 2004).

### 5.7.1 O experimento

(RIEFFEL; POLAK, 2000)

Um feixe de luz brilha em uma tela de projeção. Filtros A, B e C, onde A é polarizado horizontalmente, B a 45° e C verticalmente.) e pode ser colocado de modo a cruzar o feixe de luz. Primeiro, insira o filtro A. Supondo que a luz que entra é polarizada aleatoriamente (produza fótons com polarização aleatória), a intensidade da saída terá metade da intensidade da luz recebida. Os fótons de saída agora estão todos polarizados horizontalmente. O filtro A medirá 50% de todos os fótons polarizados horizontalmente. Estes fótons passarão pelo filtro A e seu estado serão  $|\rightarrow\rangle$ .

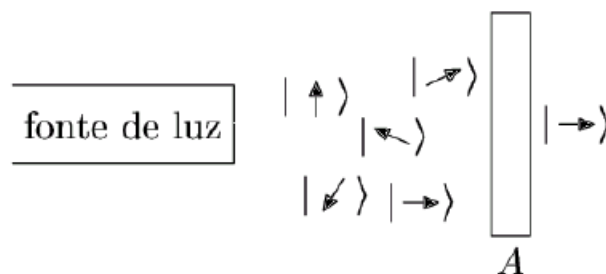


Figura 85 – Polarização de fótons - Filtro A.

Fonte: (CARDONHA; SILVA; FERNANDES, 2004)

Um fóton pode estar polarizado verticalmente (representado por  $|\uparrow\rangle$ ), horizontalmente (representado por  $|\rightarrow\rangle$ ), ou numa superposição destes estados, ou seja,  $\alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ , com  $\alpha, \beta \in \mathbb{C}$ . Assumindo que a luz gerada é aleatoriamente polarizada, cerca de metade dos fótons emitidos serão polarizados horizontalmente por A e o atravessam. Note que A deixa passar apenas os fótons com  $\alpha = 0$  e  $\beta = 1$ .

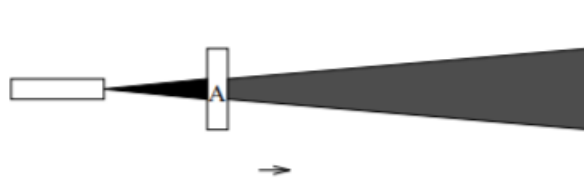


Figura 86 – Polarização de fótons - Filtro A.

Fonte: An Introduction to Quantum Computing for Non-Physicists - Eleanor Rieffel, FX Palo Alto Laboratory and Wolfgang Polak, Consultant, <[arXiv:quant-ph/9809016v2](https://arxiv.org/abs/quant-ph/9809016v2)>, Jan 19, 2000.

A função do filtro A não pode ser explicada como uma "peneira" que só permite que esses fótons passem que já estão polarizados horizontalmente. Se fosse esse o caso, poucos dos aleatoriamente fótons entrantes polarizados seriam polarizados

horizontalmente, então esperaríamos muito maior atenuação da luz à medida que passa pelo filtro.

Em seguida, quando o filtro C é inserido, a intensidade da saída cai para zero. Nenhum dos fótons polarizados horizontalmente podem passar pelo filtro vertical. Os fótons polarizados horizontalmente não passam pelo filtro vertical C. Um modelo de peneira poderia explicar esse comportamento.

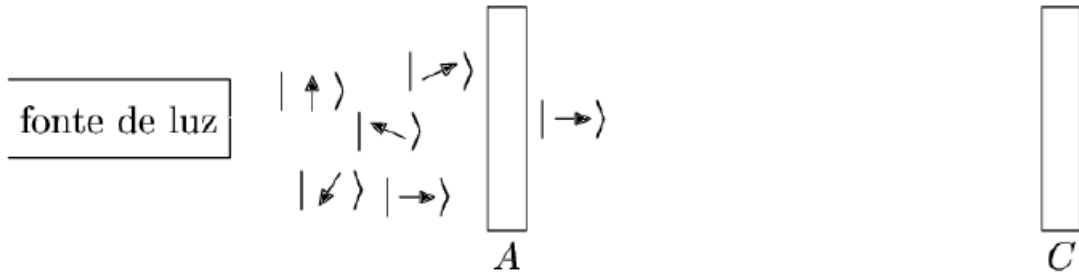


Figura 87 – Polarização de fótons inicial em A - Filtro A.

Fonte: (CARDONHA; SILVA; FERNANDES, 2004)

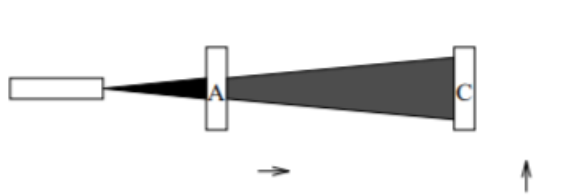


Figura 88 – Polarização de fótons - Filtros A e C.

Fonte: An Introduction to Quantum Computing for Non-Physicists - Eleanor Rieffel, FX Palo Alto Laboratory and Wolfgang Polak, Consultant, <arXiv:quant-ph/9809016v2>, Jan 19, 2000.

Porém, se adicionarmos B entre A e C, observaremos que  $1/8$  dos fótons emitidos pela fonte atravessam C (veja a Figura 90). Após o filtro B ser inserido entre A e C, uma pequena quantidade de luz será visível na tela (C), exatamente um oitavo da quantidade original de luz.

Aqui nós temos um efeito não intuitivo. A experiência clássica sugere que adicionar um filtro deveria somente ser capaz de diminuir o número de fótons passando. Como isso pode aumentar?

### 5.7.2 A explicação

O estado de polarização de um fóton pode ser modelado por um vetor unitário apontando na direção apropriada. Qualquer polarização arbitrária pode ser expressa como combinação linear  $\alpha|\uparrow\rangle + \beta|\rightarrow\rangle$  dos dois vetores base  $|\rightarrow\rangle$  (polarização horizontal) e  $|\uparrow\rangle$  (polarização vertical).

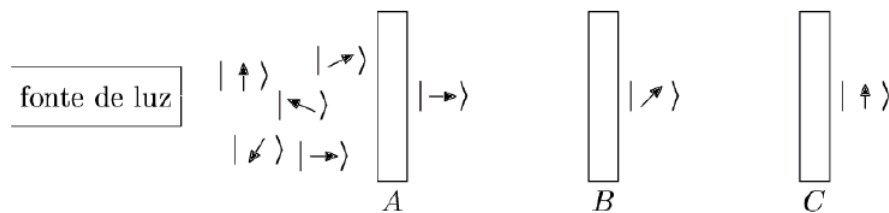


Figura 89 – Polarização de fótons - Filtros A, B e C.

Fonte: An Introduction to Quantum Computing for Non-Physicists - Eleanor Rieffel, FX Palo Alto Laboratory and Wolfgang Polak, Consultant, <arXiv:quant-ph/9809016v2>, Jan. 19, 2000.

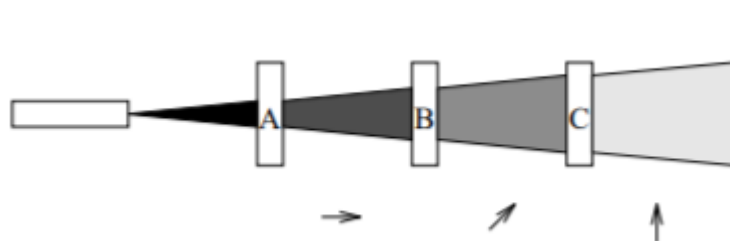


Figura 90 – Polarização de fótons - Filtros A, B e C.

Fonte: An Introduction to Quantum Computing for Non-Physicists - Eleanor Rieffel, FX Palo Alto Laboratory and Wolfgang Polak, Consultant, <arXiv:quant-ph/9809016v2>, Jan. 19, 2000.

Como estamos interessados apenas na direção da polarização (a noção de "magnitudo" não é significativa), o vetor de estado será um vetor unitário, ou seja,  $|\alpha|^2 + |\beta|^2 = 1$ . Em geral, a polarização de um fóton pode ser expressa como  $\alpha |\uparrow\rangle + \beta |\rightarrow\rangle$ , onde  $\alpha$  e  $\beta$  são números complexos tal que  $|\alpha|^2 + |\beta|^2 = 1$ . Note que a escolha da base para esta representação é completamente arbitrária: quaisquer dois vetores unitários ortogonais servirão (por exemplo,  $\{|\swarrow\rangle, |\nearrow\rangle\}$  ou  $\{|\nearrow\rangle, |\searrow\rangle\}$ ).

O postulado de medição da mecânica quântica afirma que qualquer dispositivo que meça sistema 2-dimensional tem uma base ortonormal associada em relação ao qual a medição de um estado quântico ocorre. A medição de um estado transforma o estado em um dos vetores de base associados ao dispositivo de medição. A probabilidade de que o estado seja medido como o vetor de base  $|u\rangle$  é o quadrado da norma da amplitude do componente do estado original, na direção do vetor de base  $|u\rangle$ . Por exemplo, dado um dispositivo para medir a polarização de fótons com base associada  $\{|\uparrow\rangle, |\rightarrow\rangle\}$ , o estado  $\varphi = \alpha |\uparrow\rangle + \beta |\rightarrow\rangle$  é medido como  $|\uparrow\rangle$  com probabilidade  $|\alpha|^2$  e como  $|\rightarrow\rangle$  com probabilidade  $|\beta|^2$  (veja a Figura 91). Nota que diferentes dispositivos de medição têm diferentes bases associadas e medições usando esses dispositivos terá resultados diferentes. Como as medições são sempre feitas com respeito a uma base ortonormal, durante todo o restante deste livro, todas as bases serão assumidas ser *ortonormal*.

Além disso, a medição do estado quântico mudará o estado para o resultado da medição. Isto é, se a medição de  $\varphi = \alpha |\uparrow\rangle + \beta |\rightarrow\rangle$  resultar em  $|\uparrow\rangle$ , então o estado  $\varphi$  muda para  $|\uparrow\rangle$  e uma segunda medição com relação à mesma base retornará  $|\uparrow\rangle$  com probabilidade 1. Assim, a menos que o estado original tenha sido um dos vetores



base, a medição mudará esse estado, e não é possível determinar o que o original estado era.

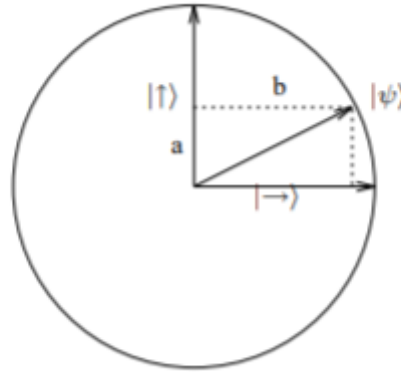


Figura 91 – Um medição - É uma projeção sobre a base, onde  $a = \alpha$  e  $b = \beta$ .

Fonte: An Introduction to Quantum Computing for Non-Physicists - Eleanor Rieffel, FX Palo Alto Laboratory and Wolfgang Polak, Consultant, <[arXiv:quant-ph/9809016v2](https://arxiv.org/abs/quant-ph/9809016v2)>, Jan 19, 2000.

A mecânica quântica explica esse fenômeno do seguinte modo. Em A, ocorre uma medição do fóton, de acordo com o observável  $O_A = \{E_1, E_2\}$ , onde  $E_1$  e  $E_2$  são gerados, respectivamente, por  $|\uparrow\rangle$  e por  $|\rightarrow\rangle$ , ele estará no estado  $|\uparrow\rangle$  com probabilidade  $|\alpha|^2$  e no estado  $|\rightarrow\rangle$  com probabilidade  $|\beta|^2$ . Apenas estes últimos, projetados sobre  $E_2$ , atravessam A.

Em C ocorre uma medição de acordo com o mesmo observável  $O$ , porém apenas os fótons projetados sobre  $E_1$  pela medição atravessam o polaróide. Se B não estiver entre A e C, todos os fótons chegando a C são da forma  $0|\uparrow\rangle + 1|\rightarrow\rangle$  e portanto não é possível que nenhum deles o atravesse.

Entretanto, caso B seja interposto entre A e C, ele realizará uma medição de acordo com o observável  $O = \{E'_1, E'_2\}$ , onde  $E'_1$  e  $E'_2$  são gerados respectivamente por  $|\nearrow\rangle$  e por  $|\searrow\rangle$ , onde

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle) \text{ e } |\searrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle).$$

Com isso, metade dos fótons polarizados horizontalmente que atingem B é projetada sobre  $E'_1$  e o atravessa, enquanto a outra metade é projetada sobre  $E'_2$  e é absorvida ou refletida.

Agora os fótons que chegam a C não terão mais  $\alpha = 0$  e  $\beta = 1$ , e sim  $\alpha = \beta = \frac{1}{\sqrt{2}}$ . Desta forma, metade deles será projetada sobre  $E_1$  e atravessará C e a outra metade é absorvida ou refletida. Assim, cerca de 1/8 do total de fótons emitidos pela fonte atravessa A, B e C, como observado experimentalmente.

Em outras palavras, como em (RIEFFEL; POLAK, 2000)

A mecânica quântica pode explicar o experimento de polarização da seguinte forma:

uma polaróide mede o estado quântico dos fótons em relação à base que consiste no vetor correspondendo à sua polarização, junto com um vetor ortogonal à sua polarização. Os fótons que, depois de medidos pelo filtro, coincidirem com a polarização do filtro são liberados. Os outros são refletidos e tem uma polarização perpendicular à do filtro. Por exemplo, o filtro A mede a polarização de fótons com relação à base vetor  $|\rightarrow\rangle$ , correspondente à sua polarização. Os fótons que passam pelo filtro A todos tem polarização  $|\rightarrow\rangle$ . Aqueles que são refletidos pelo filtro, todos têm polarização  $|\uparrow\rangle$ .

Assumindo que a fonte de luz produza fótons com polarização aleatória, o filtro A medirá 50% de todos os fótons polarizados horizontalmente. Estes fótons passarão pelo filtro A e seu estado serão  $|\rightarrow\rangle$ . O filtro C medirá esses fótons em relação a  $|\uparrow\rangle$ . Mas o estado  $|\rightarrow\rangle = 0|\uparrow\rangle + 1|\rightarrow\rangle$  será projetado em  $|\uparrow\rangle$  com probabilidade 0 e nenhum os fótons passarão pelo filtro C.

Finalmente, o filtro B mede o estado quântico em respeito à base:

$$\left\{ \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle) \right\}$$

a qual escrevemos como:

$$\{|\nearrow\rangle, |\nwarrow\rangle\}$$

Note que:

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle) \text{ e } |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$$

Aqueles fótons que são medidos como  $|\nearrow\rangle$  passam através do filtro. Fótons passando através do filtro A com  $|\rightarrow\rangle$  serão medidos pelo filtro B como  $|\nearrow\rangle$  com probabilidade  $\frac{1}{2}$  e assim 50% dos fótons passando através de A, passarão através de B e estará no estado  $|\nearrow\rangle$ .

Como anteriormente, esses fótons serão medidos pelo filtro C  $|\uparrow\rangle$  com probabilidade  $\frac{1}{2}$ . Assim, somente  $\frac{1}{8}$  do fótons originais conseguem passar através dos filtros A, B e C.

A polarização de fótons será utilizada na construção de protocolos quânticos para criptografia, como mostrado no capítulo 12.

## 5.8 Princípios da Incerteza e da Complementaridade

O *princípio da incerteza* consiste num enunciado da mecânica quântica formulado em 1927 por **Werner Heisenberg**. Tal princípio estabelece um limite na precisão com que certos pares de propriedades de uma dada partícula física, conhecidas como variáveis complementares (tais como posição e momento linear), podem ser conhecidos. Em seu artigo de 1927, **Heisenberg** propõe que em nível quântico

quanto menor for a incerteza na medida da posição de uma partícula, maior será a incerteza de seu momento linear (quantidade de movimento medido de uma partícula) e vice-versa ([HEISENBERG, 1927b](#)).

O **princípio da incerteza** é um dos aspectos mais conhecidos da física do século XX e é comumente apresentado como um exemplo claro de como a mecânica quântica se diferencia das premissas elementares das teorias físicas clássicas ([HEISENBERG, 1927a](#)). Isso porque na mecânica clássica quando conhecemos as condições iniciais conseguimos com precisão determinar o movimento e a posição dos corpos de forma simultânea. Ainda que o *princípio da incerteza* tenha sua validade restrita ao nível subatômico, ao inserir valores como indeterminação e probabilidade no campo do experimento empírico, tal princípio constitui uma transformação epistemológica fundamental para a ciência do século XX. **Gaston Bachelard** (1884-1962) é um filósofo francês, suas obras referem-se às questões ligadas à epistemologia e à filosofia da ciência. Grande parte da obra bachelariana é marcada pelo contexto da revolução científica promovida no início do século XX (1905) pela Teoria da Relatividade, formulada por **Albert Einstein** <<https://farofafilosofica.com/2018/03/11/gaston-bachelard-10-livros-para-download-em-pdf/>>.

O **princípio da complementaridade** foi enunciado por **Niels Bohr** em 1928 e assevera que: **a natureza da matéria e radiação é dual e os aspectos ondulatório e corpuscular não são contraditórios, mas complementares**. Daí vem o nome do princípio.

Isto significa que a natureza corpuscular (partícula) e ondulatória são ambas detectáveis separadamente e surgem de acordo com o tipo de experiência. Assim, na experiência da dupla-fenda a natureza evidenciada da luz é ondulatória, ao passo que **na experiência do efeito fotoelétrico, a natureza que ressalta é a corpuscular** (partícula), como demonstrou **Einstein**. Argumentos similares valem também para a matéria. Assim, o princípio da complementaridade atesta a ambiguidade e natureza dupla da matéria e energia.

## 5.9 Bibliografia e Fonte de Consulta

Experimento da dupla-fenda de Young, realizado com elétrons, <<http://www.if.ufrgs.br/historia/young.html>>, acessado em 16/10/2017.

Experiências com projéteis e ondas - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula01.pdf>>. Descrever experiências de interferência por uma fenda dupla com projéteis e ondas.

Experiências com elétrons - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula02.pdf>>. Descrever uma experiência de interferência por uma fenda dupla com partículas quânticas.

O **Princípio da Complementaridade** e o papel do observador na mecânica quântica - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula03.pdf>>. Descrever a experiência de interferência por uma fenda dupla com elétrons, na qual a trajetória destes é observada por partículas de luz (fótons).

Função de onda e Equação de Schrödinger - <<https://www.fing.edu.uy/if/cursos/>>

[fismod/cederj/aula04.pdf](#)>. Introduzir a função de onda e a Equação de Schrödinger.

Operadores *momento* e *energia* e o Princípio da Incerteza - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula05.pdf>>. Definir os operadores quânticos do *momento linear* e da *energia* e enunciar o **Princípio da Incerteza de Heisenberg**.

Momento linear (quantidade de movimento) - Helerbrock, Rafael. "O que é momento linear?"; Brasil Escola. Disponível em <<https://brasilecola.uol.com.br/o-que-e/fisica/o-que-e-momento-linear.htm>>. Acesso em 24 de abril de 2019.

## 5.10 Referências e Leitura Recomendada

José Leite Lopes, *A estrutura quântica da matéria - do átomo pré-socrático às partículas elementares*, UFRJ, Editora/Academia Brasileira de Ciências/ERCA-Editora e Gráfica limitada - Rio de Janeiro

Heisenberg, W. (1927), "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik", *Zeitschrift für Physik* (in German), 43 (3-4): 172-198, Bibcode:1927ZPhy...43..172H, doi:10.1007/BF01397280.. Annotated pre-publication proof sheet of Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, March 21, 1927.

"The uncertainty principle", in. *Stanford Encyclopedia of philosophy*. Disponível em: <https://plato.stanford.edu/entries/qt-uncertainty/>

BACHELARD, G. in *L'expérience de l'espace dans la physique contemporaine*. Paris, Felix Alcan, 1997.

O caso estacionário em uma dimensão - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula06.pdf>>. Aplicar o formalismo quântico no caso de o potencial ser independente do tempo.

A partícula livre - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula07.pdf>>. Estudar o movimento de uma partícula quântica livre, ou seja, aquela que não sofre a ação de nenhuma força.

O degrau de potencial. Caso I: energia menor que o degrau - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula08.pdf>>. Aplicar o formalismo quântico ao caso de uma partícula quântica que incide sobre um potencial  $V(x)$  que tem a forma de um degrau, ou seja, tem um valor 0 para  $x < 0$  e um valor  $V_0 > 0$  para  $x > 0$ . Vamos considerar inicialmente o caso em que a energia da partícula é menor que a altura do degrau.

O degrau de potencial. Caso II: energia maior que o degrau - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula09.pdf>>. Aplicar o formalismo quântico ao caso de uma partícula quântica que incide sobre o degrau de potencial, definido na Aula 8. Vamos considerar agora o caso em que a energia da partícula é maior que a altura do degrau.

Exercícios - <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula10.pdf>>. Aplicar o formalismo quântico estudado neste módulo à resolução de um conjunto de

exercícios.

A barreira de potencial: casos  $E < V_0$  e  $E > V_0$ . <<https://www.fing.edu.uy/if/cursos/fismod/cederj/aula11.pdf>>. Aplicar o formalismo quântico ao caso de uma partícula que incide sobre uma barreira de potencial, em que a energia potencial tem um valor 0 para  $x < 0$  e para  $x > a$ , e um valor  $V_0 > 0$  para  $0 < x < a$ .

S. Gerlich, S. Eibenberger, M. Tomandl, S. Nimmrichter, Klaus Hornberger, Paul J. Fagan, Jens Tüxen, Marcel Mayor, Markus Arndt - Quantum interference of large organic molecules, - Nature communications, 2011.

Parte II  
A Matemática



# A Base Matemática Algébrica

Neste capítulo, as formulações matemáticas são os formalismos matemáticos que permitam uma descrição rigorosa da mecânica quântica. Estas, por sua vez, se distinguem do formalismo matemático da mecânica clássica, pelo uso de estruturas matemáticas abstratas, tais como os **Espaços de Hilbert** de dimensão infinita e *operadores* sobre estes espaços.

Muitas destas estruturas são retiradas da Análise Funcional, uma área de pesquisa dentro Matemática que foi influenciada, em parte, pelas necessidades da *mecânica quântica*. Em resumo, os valores físicos observáveis, tais como *energia* e *momento* já não eram considerados como valores de funções em um *Espaço de Fase* - a representação das variáveis dinâmicas relevantes de um sistema; uma trajetória no espaço de fase representa a evolução temporal do sistema, através da evolução temporal de suas variáveis relevantes. O Espaço de Fase é uma ferramenta útil na compreensão do comportamento dos sistemas - mas como *autovalores*, mais precisamente: como valores espectrais de *operadores lineares* nos **Espaços de Hilbert** como em (AMARAL, 2006).

## 6.1 Análise Funcional

A *Análise Funcional* é o ramo da matemática, e mais especificamente da Análise Matemática, que trata do estudo de *espaços de funções*. Tem suas raízes históricas no estudo das *transformações*, tais como a *Transformada de Fourier*, e no estudo de *equações diferenciais* e *equações integrais*.

A palavra *funcional* remonta ao *Cálculo das Variações*, implicando uma função cujo argumento é uma função. Em matemática, em especial na *Álgebra linear* e *Análise Matemática*, define-se como um *funcional*, toda função cujo domínio é um espaço vetorial e a imagem é um *corpo* de escalares. Intuitivamente, pode-se dizer que um *funcional* é uma "função de uma função".

**Definição** (O que é um Funcional)

Em matemática, define-se como um **funcional**, toda função cujo domínio é um **espaço vetorial** e a imagem é o **corpo de escalares** que define o mesmo espaço.



Intuitivamente, pode-se dizer que um **funcional** é uma "função de uma função".

Seja  $\mathbb{V}$  um espaço vetorial sobre um corpo  $\mathbb{K}$ , então um **funcional** é qualquer função  $\mathbb{V} \rightarrow \mathbb{K}$ . O conjunto  $\mathbb{V}$ , o domínio, é uma classe de funções. O conjunto de números reais associados com as funções em  $\mathbb{V}$  é chamado de conjunto imagem do funcional. Como este espaço vetorial  $\mathbb{V}$  (domínio de um funcional) geralmente é de funções, há outra definição específica para este caso:

Um *funcional*  $\Phi$  é uma regra de correspondência que associa a cada função  $f$  em uma certa classe  $\mathbb{V}$  um único número real.

**Exemplo** (Funcional de  $\mathbb{R}^2 \rightarrow \mathbb{R}$ )

Considere  $\mathbb{R}^2$  sobre o corpo dos números reais, onde cada vetor pode ser denotado por  $\mathbf{x} = (x_1, x_2)$ . Eis alguns exemplos de *funcionais*:

$$\begin{aligned} l_1(\mathbf{x}) &= x_1 \\ l_2(\mathbf{x}) &= x_2 \\ l_3(\mathbf{x}) &= \|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2} \\ l_4(\mathbf{x}) &= \mathbf{x} \cdot \mathbf{y} = x_1 y_1 + x_2 y_2, \end{aligned}$$

onde  $\mathbf{y} = (y_1, y_2)$  é um vetor dado.

Um *funcional* é dito *funcional linear* se for linear, ou seja, se  $\alpha$  e  $\beta$  são escalares:

$$l(\alpha x + \beta y) = \alpha.l(x) + \beta.l(y)$$

O *Cálculo das Variações* resolve o problema matemático que consiste em buscar máximos e mínimos (ou, mais geralmente, extremos relativos) de funções contínuas definidas sobre algum *espaço funcional*. Constitue uma generalização do *Cálculo ordinário* de máximos e mínimos de funções reais de uma variável. Ao contrário deste, o *Cálculo das Variações* lida com os *funcionais* (funções de funções), enquanto o cálculo ordinário trata de *funções*.

*Funcionais* podem, por exemplo, ser formados por *integrais* envolvendo uma função incógnita e suas derivadas. O interesse está em *funções extremas* - aquelas que fazem o *funcional* atingir um valor máximo ou mínimo - ou de *funções fixas* - aquelas onde a taxa de variação do funcional é precisamente zero.

Um grande impulso para o avanço da *Análise Funcional* durante o século XX foi a *modelagem da mecânica quântica* em **Espaços de Hilbert**, devida a **John von Neumann**.

O leitor pode ler sobre **John von Neumann** (matemático, lógico e ciência da computação) e **David Hilbert** (matemático, idealizador do que se chama *formalismo*), nos capítulos referentes a eles no volume I (Dos Primórdios da Matemática aos Sistemas Formais), nesta mesma série. Para entendimento destas áreas da Matemática, as disciplinas de Cálculos (I, II, III, IV) como são ensinadas em cursos de graduação, são muito bem-vindas. Mas, como ressaltadas no Capítulo I do Volume I desta série, fazem parte da base matemática para se estudar os *sistemas contínuos*, não considerados nos volumes I e II, os quais tratam da *matemática dos sistemas*

*discretos.*

Talvez a melhor contribuição para a Matemática tenha sido os **Espaços de Hilbert**. Esses são uma generalização do conceito de espaço euclidiano, mas que não precisam estar restrito a um número finito de dimensões. É um espaço vetorial dotado de produto interno, ou seja, com noções de distância e ângulos. Os **Espaços de Hilbert** permitem que, de certa maneira, noções intuitivas sejam aplicadas em espaços funcionais (de funções). Os **Espaços de Hilbert** são de importância crucial para a *mecânica quântica*.

Álgebra abstrata é a sub-área da matemática que estuda as estruturas algébricas como grupos, *anéis*, *corpos*, *espaços vetoriais* e álgebras em geral. O termo abstrata é utilizado para diferenciar essa área da álgebra elementar estudada no ensino fundamental, na qual são abordadas regras para manipular (somar, multiplicar, ...) expressões algébricas em que aparecem variáveis e números reais ou complexos. A álgebra abstrata é estudada em Matemática, mas também é utilizada na Física e Ciência da Computação.

## 6.2 Teoria dos Grupos algébricos

Em Matemática (Álgebra), teoria dos grupos é o ramo que estuda as estruturas algébricas chamadas de **grupos**. De outra forma - "Teoria dos grupos é o ramo da matemática que responde à questão: O que é **simetria**?"

O conceito de **grupo** é fundamental para a álgebra abstrata: outras bem conhecidas estruturas algébricas, como os **anéis**, **corpos**, e espaços vetoriais.

A **teoria de Galois**, que é a origem histórica do conceito de grupo, procura descrever as simetrias das equações satisfeitas pelas soluções de uma equação polinomial.

Grupos abelianos (comutativos) estão presentes em várias estruturas estudadas em álgebra abstrata, como anéis, corpos, e módulos.

Grupos são usados na Matemática e nas ciências em geral para capturar a simetria interna de uma estrutura na forma de automorfismos de grupo. Uma simetria interna está normalmente associada com alguma propriedade invariante, e o conjunto de transformações que preserva este invariante, juntamente com a operação de composição de transformações, forma um grupo chamado um grupo de simetria.

Na topologia algébrica, grupos são usados para descrever os invariantes de espaços topológicos. Eles são chamados de "invariantes" porque não mudam se o espaço é submetido a uma transformação. Exemplos incluem o grupo fundamental, grupo de homologias e o grupo de cohomologias.

Os **grupos algébricos lineares** e os **grupos de Lie** são dois ramos da teoria dos grupos que experimentaram enormes avanços e por isso são estudados como sub-matérias de maior importância.

O conceito de **grupo de Lie** (em homenagem ao matemático Sophus Lie) é importante no estudo de equações diferenciais em variedades; ele combina análise e

teoria de grupos e é portanto a ferramenta certa para descrever as simetrias das estruturas analíticas. Análise neste e outros grupos é chamada de análise harmônica. A análise harmônica é o ramo da matemática que estuda a representação de funções ou sinais como a sobreposição de ondas base. Ela investiga e generaliza as noções das séries de Fourier e da transformação de Fourier. As ondas básicas são chamadas de harmônicas, e este ramo da matemática logo passou a ser conhecido pelo nome de "análise harmônica". Nos dois séculos passados (XIX e XX), tornou-se um tema vasto, com aplicações em áreas tão diversas como o processamento de sinais, **mecânica quântica**, e ciência neuronal.

Na **análise combinatória**, a noção de grupo de permutação e o conceito de ação de um grupo são frequentemente utilizados para simplificar a contagem de um conjunto de objetos.

A compreensão da teoria de grupos é fundamental na Física, onde é utilizada para descrever as simetrias que as leis da Física devem obedecer. O interesse da Física na representação de grupos é grande, especialmente em **grupos de Lie**, pois suas representações podem apontar o caminho para "possíveis" teorias físicas. Em Química, **grupos** são utilizados para classificar **estruturas cristalinas** e a simetrias das moléculas.

Uma das mais importantes realizações matemáticas do século XX foi o esforço colaborativo, que ocupou mais de 10.000 páginas de periódicos na maior parte publicados entre 1960 e 1980, e que culminou na completa classificação dos **grupos finitos**, utilizados em curvas elípticas aplicadas à segurança computacional em algoritmos de criptografia.

**Definição** (O que é um grupo)

Seja  $G$  um conjunto e considere  $*$  uma operação binária definida sobre  $G$ . O par ordenado  $(G, *)$  é um **grupo**, se são satisfeitas as seguintes propriedades:

**(Associatividade)** - Quaisquer elementos  $a, b, c$  pertencentes a  $G$ , tal que  $(a * b) * c = a * (b * c)$  e  $(a * b) * c = a * (b * c)$ .

**(Existência do elemento neutro)** - Existe um elemento  $e$  em  $G$  tal que  $e * a = a * e = a$  e  $e * a = a * e = a$ , para todo  $a$  pertencente a  $G$ .

**(Existência do elemento simétrico)** - Para qualquer elemento  $a$  em  $G$ , existe outro elemento  $a'$  em  $G$ , tal que,  $a * a' = a' * a = e$ , onde  $e$  é o *elemento neutro* previamente mencionado.

É possível denominar por grupo um conjunto  $G$ , desde que a operação em questão esteja evidente. Veja a Figura 92.

**Definição** (Ordem em um grupo)

A ordem de um grupo  $(G, *)$ , onde  **$G$  é finito**, é o número de elementos do conjunto  $G$ .

**Exemplos** (Grupos)

- O menor grupo é formado por um único elemento.

Operação	Símbolo da operação	Elemento neutro	Elemento	Simétrico de um elemento
Adição	+	0 (Zero)	a	-a (Oposto de a)
Multiplicação	.	1 (Um)	a	$a^{-1}$ (Inverso de a)
Composição de funções	o	$i(x)=x$ (identidade)	$a(x)$	$a^{-1}(x)$ (Função inversa de $a(x)$ )

Figura 92 – Denominações em determinados grupos.

Fonte: <[https://pt.wikipedia.org/wiki/Grupo\\_\(matemática\)](https://pt.wikipedia.org/wiki/Grupo_(matemática))>

- O conjunto  $\{1,-1\}$  é um grupo relativamente à multiplicação usual.
- O conjunto de todas as bijecções do conjunto  $\{1,2,\dots,n\}$  em si próprio é um grupo se, se considerar como operação binária a composição. Este grupo representa-se por  $S_n$ . Ver abaixo um detalhamento deste exemplo.
- Um exemplo de grupo de ordem finita é o **grupo Klein**,  $G = \{e, a, b, c\}$ , onde  $e$  é o elemento neutro, todo elemento é seu próprio inverso, e as demais operações são definidas de forma que se  $x, y$  e  $z$  são três elementos distintos, então  $x * y = z$  e  $x * y = z$ .
- O conjunto  $(\mathbb{Z}_n, +)$  formado pelos números entre 0 e  $n-1$ , em que a soma é feita *módulo*  $n$ , é um grupo. Por exemplo, em  $(\mathbb{Z}_{42}, +)$ , temos que  $20 + 30 = 50 \bmod 42 = 8$ .
- O grupo de simetrias de um polígono regular de  $n$  lados, chamado  $D_n$  ou *grupo diedral*. Ver abaixo um detalhamento deste exemplo.
- O conjunto  $M_n(\mathbb{R})$  das matrizes quadradas de ordem  $n$ , não forma um grupo sob a multiplicação de matrizes, uma vez que a matriz nula, por exemplo, não admite um inverso. No entanto, o subconjunto  $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$  é um grupo sob a multiplicação.
- O conjunto das matrizes da forma:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

onde  $a, b$  e  $c$  são número reais, forma grupo com a multiplicação usual de matrizes. Esse é o chamado **Grupo de Heisenberg**.

## 6.3 Grupo e Simetrias

**Grupos das Simetrias de um quadrado** - Quando construimos polígonos regulares, podemos ordenar os seus vértices para formar uma espécie de referência. Seja um polígono regular de ordem  $n$ . Ao considerarmos apenas as diversas configurações que não alteram o formato do polígono - modificando, portanto, somente as posições de seus vértices - temos o conjunto diedral de ordem  $n$  (representado por  $D_n$ ). A seguir, as possíveis configurações de um quadrado na Figura 93:

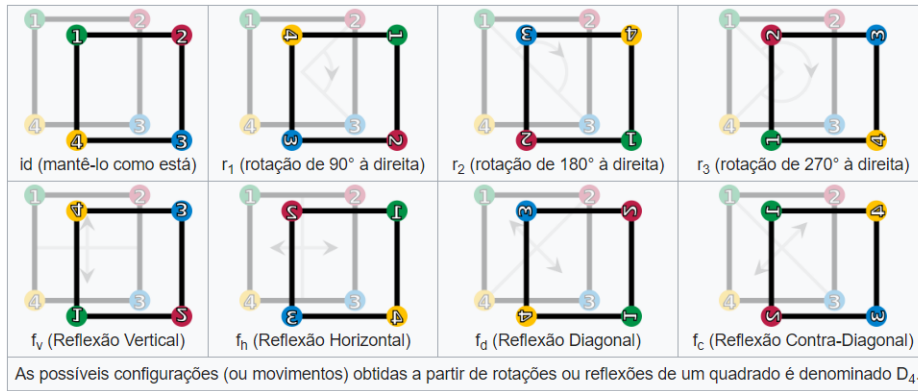


Figura 93 – Simetrias de um quadrado.

Fonte: <[https://pt.wikipedia.org/wiki/Grupo\\_\(matemática\)](https://pt.wikipedia.org/wiki/Grupo_(matemática))>

Estabelecendo a operação  $*$  sobre este conjunto, definida por:  $a, b \in D_n, a * b = c$ , onde  $c$  é a configuração obtida após executar o movimento  $a$  e em seguida o movimento  $b$ .

A partir da operação entre quaisquer elementos de  $D_4$ , é possível verificar que o resultado também é um elemento de  $D_4$ . Por exemplo,  $r_1 * r_1 = r_2, f_v * f_v = id$ . Como  $D_4$  se trata de um conjunto finito, é perfeitamente possível construir uma tabela (Tabela de Cayley) conforme a Tabela 94, com os resultados da operação entre quaisquer dois de seus elementos.

**Tábua de Cayley de  $D_4$**

•	id	$r_1$	$r_2$	$r_3$	$f_v$	$f_h$	$f_d$	$f_c$
id	id	$r_1$	$r_2$	$r_3$	$f_v$	$f_h$	$f_d$	$f_c$
$r_1$	$r_1$	$r_2$	$r_3$	id	$f_c$	$f_d$	$f_v$	$f_h$
$r_2$	$r_2$	$r_3$	id	$r_1$	$f_h$	$f_v$	$f_c$	$f_d$
$r_3$	$r_3$	id	$r_1$	$r_2$	$f_d$	$f_c$	$f_h$	$f_v$
$f_v$	$f_v$	$f_d$	$f_h$	$f_c$	id	$r_2$	$r_1$	$r_3$
$f_h$	$f_h$	$f_c$	$f_v$	$f_d$	$r_2$	id	$r_3$	$r_1$
$f_d$	$f_d$	$f_h$	$f_c$	$f_v$	$r_3$	$r_1$	id	$r_2$
$f_c$	$f_c$	$f_v$	$f_d$	$f_h$	$r_1$	$r_3$	$r_2$	id

Os elementos id,  $r_1, r_2$  e  $r_3$  formam um subgrupo de  $D_4$ , colorido em vermelho. Em verde e amarelo, classes laterais esquerda e direita desse subgrupo, respectivamente.

Figura 94 – Tabela de Cayley das simetrias de um quadrado.

Fonte: <[https://pt.wikipedia.org/wiki/Grupo\\_\(matemática\)](https://pt.wikipedia.org/wiki/Grupo_(matemática))>

Com o auxílio desta tabela, verificamos as seguintes propriedades de  $D_4$  em relação a operação  $*$ :

- Para quaisquer elementos  $a, b$  e  $c$  de  $D_4, (a * b) * c = a * (b * c)$ .

- Existe um elemento  $e$  que, operado a qualquer outro elemento  $y$ , resulta em  $y$  ou seja:  $\exists e \in D_4 : \forall y \in D_4, e * y = y * e = y$ .
- Para todo elemento  $x \in D_4$  portando a ordem) resultam no elemento  $e$  do item anterior, ou seja:  $\forall x \in D_4, \exists x' : x * x' = x' * x = e$ .

Claramente, o elemento  $e$  em questão é  $id$ , pois ao operá-lo a qualquer elemento, o mesmo não tem sua configuração alterada. A terceira propriedade é verificada nas linhas e colunas da tabela dos possíveis resultados da operação  $*$  em relação aos elementos de  $D_4$ . Em cada linha e cada coluna, verificamos que o elemento  $id$  aparece uma única vez. Portanto, para qualquer elemento  $x$ , existe outro elemento  $x'$  que, operado ao primeiro, resulta em  $id$ .

### Propriedades Imediatas

1. A identidade de um grupo é única.
2. Um elemento de um grupo  $G$  possui apenas um inverso.
3. Em um grupo temos  $(xy)^{-1} = y^{-1}x^{-1}$ .

## 6.4 Teoria dos Anéis algébricos

Em Matemática, a teoria de anéis é o estudo das estruturas algébricas com duas operações binárias, por exemplo, uma adição '+' e uma multiplicação '.', e que possuem propriedades similares às dos números inteiros.

O estudo de **anéis** originou-se da teoria de anéis de polinômios e da teoria de inteiros algébricos. **Richard Dedekind** foi quem introduziu o conceito de anel e também introduziu o conceito de **ideal**, baseado na noção de **anel**, por volta de 1879. O termo **anel** (Zahlring) foi criado por **David Hilbert** no artigo *Die Theorie der algebraischen Zahlkörper*, *Jahresbericht der Deutschen Mathematiker Vereinigung*, Vol. 4, 1897. A primeira definição axiomática de anéis foi dada por **Adolf Fraenkel** em um ensaio no *Journal für die reine und angewandte Mathematik* (A. L. Crelle), vol. 145, 1914. Em 1921, **Emmy Noether** criou a primeira base axiomática da teoria de anéis comutativos em seu monumental trabalho *Ideal Theory in Rings*.

### Definição (Anel)

Dado um conjunto  $A$  e duas operações binárias, dizemos que a estrutura algébrica  $(A, +, \cdot)$  forma um **anel** se:

1. Operação de adição (+) é associativa e comutativa.
2. Existe um elemento neutro na adição, chamado de 0.
3. Existe um elemento inverso para a adição, escrito como  $-x$ .
4. A operação de multiplicação (.) é associativa.
5. A operação de multiplicação se distribui sobre a adição:  
 $a \cdot (b + c) = a \cdot b + a \cdot c$ ,  $\forall a, b, c \in S$  (distributividade).

Um **anel** que também possua um elemento neutro com relação à multiplicação é chamado de anel com unidade. Alguns autores incluem este axioma na definição de anel.

Um **anel** é chamado **anel sem divisores de zero** se:

$$\forall a, b \in A \quad a \cdot b = 0, \text{ então } a = 0 \text{ ou } b = 0.$$

Note que a estrutura  $(A, +)$  forma um **grupo abeliano** (grupo comutativo).

**Exemplo:** (Anel com divisor de zero)

O conjunto de matrizes reais  $2 \times 2$ , juntamente com as operações de adição e multiplicação de matrizes usuais, fornece um exemplo de **anel com divisor de zero**:

Neste anel de matrizes reais  $2 \times 2$ , a unidade 1 é representada pela matriz, e o elemento 0 é representada pela matriz nula, como seguem:

$$\text{Unidade } 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Zero } 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

**Divisor de zero:** seja  $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  e  $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ , então  $a \cdot b = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ , mas nem  $a$  ou  $b$  são iguais a zero (matrizes nulas).

## 6.5 John von Neumann e a Teoria de Álgebra de Operadores

O texto aqui é parte do trabalho em (EXEL, 1996), que baseado na "Obra e o Legado de John von Neumann", organizou em 1995, na USP, um evento em homenagem ao gênio de **John von Neumann**. Um **operador** pode ser definido, informalmente, como sendo uma regra que transforma uma função em outra, no contexto da área da Matemática chamada de Análise Funcional. A **teoria algébrica dos operadores** é extensa, mas aqui é colocado o que a introduz, no sentido de justificar seu uso, aplicado à **teoria quântica** por **John von Neumann**.

Respondendo a um questionário elaborado pela *National Academy of Sciences* dos EUA, **John von Neumann** considerou seu trabalho em teoria de operadores como uma de suas três contribuições científicas mais importantes. Este trabalho, iniciado no final da década de 20, tem origem no seu interesse em obter uma formalização matematicamente precisa para diversas teorias emergentes na época, dentre as quais se destaca a **mecânica quântica**.

No que veio a constituir aproximadamente um terço de sua extensa lista de publicações, **John von Neumann** desenvolveu sua **teoria de operadores nos espaços de Hilbert**, criando assim, não apenas uma nova teoria matemática, que comporta aplicações à teoria de representações de grupos infinitos, mas uma nova forma de

pensamento, que permite modelar a lógica da mecânica quântica e que, com os avanços subsequentes, proporcionou uma abrangente unificação de diversos campos da matemática. As portas abertas pelo seu trabalho continuam a provocar desenvolvimentos cruciais na fronteira da matemática dos dias de hoje.

**Von Neumann** rapidamente reconheceu que o estudo de operadores em **espaços de Hilbert** requeria um ponto de vista mais amplo, no qual vários operadores deveriam ser estudados em conjunto, e que as relações algébricas entre esses mereceriam, talvez, mais atenção que o estudo das características que cada operador apresentava isoladamente. Entretanto, não se deve ignorar a importância de seu trabalho no estudo de *single operator theory*, sendo **von Neumann** um dos criadores do importantíssimo **teorema espectral para operadores ilimitados**.

Em 1929, no artigo *Zur Algebra der Funktionaloperatoren und Theorie der normalen Operatoren*, **John von Neumann** iniciou seu estudo da **teoria dos anéis de operadores**, que hoje em dia, muito propriamente, são chamados de *Álgebras de von Neumann*. O conceito formal de *anel*, que surgiu pela primeira vez em 1921 com **Emmy Noether**, em artigo no *Mathematische Annalen*, foi imediatamente reconhecido como uma criação de fundamental importância na formulação da matemática moderna e, com **von Neumann**, ganhou alguns de seus mais importantes exemplos.

As teorias axiomáticas em Matemática muitas vezes permitem que se obtenha, de forma relativamente simples, uma classificação completa dos objetos de estudo, a exemplo da teoria dos espaços vetoriais: um espaço vetorial fica inteiramente determinado, uma vez que sua dimensão seja conhecida. Por outro lado, outras teorias tratam de objetos tão gerais, que uma classificação completa é reconhecidamente impossível. São raras as vezes em que um sistema de axiomas define um conjunto de objetos matemáticos que sejam sofisticados e gerais o suficiente para fazer, de seu estudo, um frutífero desafio intelectual, ao mesmo tempo que demarquem um terreno definido o suficiente para suscitar a possibilidade de classificação de todos os seus modelos possíveis. A **teoria dos grupos de Lie** vem à mente como um exemplo significativo. A análise cuidadosa da conexão misteriosa entre as ciências naturais e a Matemática é, frequentemente, o melhor meio para que o intelecto humano possa vir a formular tais teorias. A **teoria das álgebras de von Neumann** é um exemplo importante deste método de criação intelectual, sendo a **mecânica quântica** seu ponto de conexão com o universo físico.

Uma **álgebra de Von Neumann**, tecnicamente falando, é uma coleção  $\mathcal{M}$  de operadores limitados no **espaço de Hilbert**, aqui denotado por  $\mathcal{H}$ , que, em primeiro lugar, forma uma subálgebra da álgebra  $\mathcal{L}(\mathcal{H})$  de todos os operadores limitados em  $\mathcal{H}$ . Em segundo lugar, requer-se que seja *auto-adjunta*, ou seja, *que contenha o adjunto de cada um dos seus elementos* e, finalmente, que seja fechada na topologia forte, isto é, na topologia da convergência pontual de operadores.

De fundamental importância para os estágios iniciais do desenvolvimento da **teoria das álgebras de von Neumann**, é a série de quatro artigos intitulados *On Rings of Operators* (1936: 116-229; 1937: 208-248; 1940:96-161; 1943:716-808), em três dos quais **von Neumann** contou com a importante contribuição de **F. J. Murray**.

Já foi dito que a motivação de **von Neumann**, no seu estudo de operadores, foi entre outras, a tentativa de estabelecimento de uma base formal para a mecânica



quântica. Entretanto, os observáveis físicos são frequentemente ilimitados, o que faz com que os operadores ilimitados sejam objeto de grande interesse. Por outro lado, a teoria de álgebras de **Von Neumann** trata de operadores limitados, já que, em caso contrário, as propriedades algébricas tornam-se de difícil compreensão. Por exemplo, dados operadores ilimitados  $T_1$  e  $T_2$  não é, de forma alguma óbvia, como obter a soma  $T_1 + T_2$ . O problema que se coloca é que os domínios de  $T_1$  e  $T_2$  podem ter intersecção vazia. Entretanto, em Física quântica, manipulações formais com operadores ilimitados são rotineiramente executadas, e a utilidade destes cálculos é inegável. **Murray** e **von Neumann** obtiveram um sucesso importante no sentido de atribuir significado matemático para cálculos com operadores ilimitados.

**Definição:** (Operador Limitado)

Um operador  $A : D(A) \subseteq \mathcal{H} \rightarrow \mathcal{H}$  é chamado de **limitado** quando existe  $k \in \mathbb{R}, k > 0$ , tal que para todo  $f \in D(A)$ , temos que  $\|Af\| \leq k\|f\|$ . A norma do operador  $A$  é o número que se indica por  $\|A\|$ , e definido por:

$$\|A\| = \sup \left\{ \|f\| \mid f \in D(A) \mid f \neq 0, \frac{\|Af\|}{\|f\|} \right\}.$$

Um operador  $A$  é chamado de **ilimitado** quando **não é limitado** (AMARAL, 2006).

## 6.6 Teoria de anéis de polinômios

O anel de polinômios com *coeficientes* em um anel qualquer e qualquer *número de indeterminadas* (são as incógnitas  $x, y, \dots$ ) é a generalização dos anéis em  $\mathbb{R}[x]$ , dos polinômios com coeficientes reais  $p(x) = a_0 + a_1x + \dots + a_nx^n$ .

De forma genérica, para definir-se o *anel dos polinômios* precisa-se:

- um anel  $A$  dos coeficientes,
- um conjunto  $S$  das indeterminadas.

As indeterminadas aqui tem um significado puramente abstrato, não sendo exigido que  $S$  tenha nenhuma estrutura. Assim, é conveniente que  $S$  seja um conjunto de símbolos, e (para evitar ambiguidades) que seja disjunto de  $A$ .

Um polinômio com coeficientes em  $A$  e indeterminadas em  $S$  pode ser:

- O polinômio nulo, denominado  $0$  (exceto quando haja necessidade de fazer alguma diferença entre este polinômio e o elemento neutro de  $A$ ; neste caso, podem-se usar índices para marcar a diferença entre eles:  $0_A$  e  $0_A[S]$ )
- Os monômios, que são representados pela justaposição de um elemento (não-nulo) de  $A$  seguido de um número finito de elementos de  $S$  (podendo ser nenhum) elevados a uma potência inteira positiva. Por exemplo, se  $2 \in A$  e  $S = \{x, y\}$ , então  $2, 2x^1$  e  $2x^2y^3$  são monômios. Aqui é importante notar que os produtos de potências de  $S$  comutam, por exemplo,  $2x^2y^3 = 2y^3x^2$ . Quando a potência for 1, representa-se o monômio sem este valor:  $2x^2y^1 = 2x^2y$ .

- Uma soma de dois ou mais monômios (mas sempre uma quantidade finita), em que a parte indeterminada de todas parcelas são diferentes. Novamente, esta soma é comutativa, de forma que duas somas que diferem por uma permutação das parcelas são iguais. O anel de polinômios é este conjunto  $A[S]$  com duas operações de soma de polinômios e produto de polinômios, definidas de forma que: o polinômio nulo é elemento neutro aditivo,  $A[S]$  é um anel, o produto de monômios se comporta como se as indeterminadas comutassem entre si, e que o produto de  $x^n$  com  $x^m$  seja  $x^{n+m}$ .

*Anéis de Polinômios* consistem basicamente em traduzir fórmulas de uma lógica em polinômios com coeficientes num corpo finito (ou corpo de **Galois**), e realizar deduções através de operações sobre esses polinômios. Através da introdução de variáveis ocultas, podem ser definidos anéis de polinômios para lógicas não-caracterizáveis por matrizes finitas, como é o caso da *lógica paraconsistente mbC* e a *lógica modal S5* (CARNIELLI, 2010).

## 6.7 Polinômios de Hermite

Os **polinômios de Hermite** tem uma grande importância na mecânica quântica, mecânica que trabalha com fenômenos microscópicos. É usada a **equação de Schrodinger** independente do tempo, para a aplicação de tal modelo. De acordo com **Schrödinger** mesmo que uma partícula se mova em uma *trajetória* definida ela estará distribuída no espaço como uma *onda*. Neste sentido, uma **onda** na mecânica quântica equivaleria ao conceito de *trajetória* na mecânica clássica e seria representada por uma **função de onda**  $\psi(x)$ . Não precisando entrar em todos os detalhes destes polinômios, o leitor pode ver uma explicação detalhada em (GOUVEIA, 2014).

## 6.8 Corpos Algébricos

A *Teoria dos Corpos* é um ramo da álgebra abstrata que estuda as propriedades de estruturas algébricas chamadas *corpos*. Um corpo é uma estrutura algébrica em que a adição, a subtração, a multiplicação e a divisão são bem-definidas.

Os *corpos* são importantes objetos de estudo na Álgebra, visto que constituem uma generalização útil de muitos sistemas de números, como os números racionais  $\mathbb{Q}$ , os números reais  $\mathbb{R}$  e os números complexos  $\mathbb{C}$ . Em particular, as regras usuais de associatividade, e comutatividade e distributividade valem numa estrutura alébrica de *corpo*.

### História (Corpos Algébricos)

O conceito de *corpo* foi usado implicitamente por **Niels Henrik Abel** e **Évariste Galois** em seus trabalhos sobre resolução de raízes de equações.

Em 1871, **Richard Dedekind** deu o nome de *corpo* a um conjunto de números reais ou complexos que são fechados para as quatro operações aritméticas.

Em 1881, **Leopold Kronecker** definiu aquilo a que chamou "domínio de racionalidade", e que hoje é geralmente conhecido como "*corpo de polinômios*".

Em 1893, **Heinrich Weber** deu a primeira definição clara de um *corpo abstrato*.

Em 1910, **Ernst Steinitz** publicou o influente artigo *Algebraische Theorie der Körper* (alemão: Teoria Algébrica dos Corpos). Neste artigo ele estuda axiomaticamente as propriedades dos corpos algébricos e define conceitos importantes da teoria dos corpos, como *corpo primo*, *corpo perfeito* e o grau de transcendência de uma extensão de corpo.

**Galois** é reconhecido como o primeiro matemático a unificar a **teoria dos grupos** e a **teoria dos corpos**, originando a designação **teoria de Galois**. No entanto, foi **Emil Artin**, quem primeiro desenvolveu a relação entre *grupos* e *corpos* de forma mais desenvolvida 1928-1942.

A *teoria dos corpos* é um ramo da álgebra abstrata que estuda as propriedades dos corpos. Um *corpo* é uma estrutura algébrica em que a adição, a subtração, a multiplicação e a divisão são bem-definidas. Os corpos são importantes objetos de estudo na álgebra, visto constituírem uma generalização útil de muitos sistemas de números, como os números racionais, os números reais e os números complexos. Em particular, as regras usuais de associatividade, e comutatividade e distributividade valem nestes conjuntos numéricos.

O estudo de corpos numéricos algébricos e, mais geralmente, das extensões algébricas do corpo dos números racionais, é o tema central da *teoria algébrica dos números*.

Um corpo numérico algébrico (ou, simplesmente, corpo numérico) é uma extensão de corpo de grau finito do *corpo dos números racionais*.

**Definição** (O que é um Corpo algébrico)

Um corpo  $\mathbb{K}$  é um anel comutativo  $(K, +, \Delta)$  de tal forma que:

- $1 \in \mathbb{K}$ , com  $1 \neq 0$ ;
- $\forall k \in \mathbb{K}, k \neq 0, \exists k^{-1} \in \mathbb{K}$ , tal que  $k \Delta k^{-1} = 1$ .

Se  $\mathbb{K}$  é um corpo, então  $\mathbb{K}^* := \mathbb{K} - 0$  com a operação  $\cdot$  é um grupo abeliano (comutativo).

**Exemplos:**

- Os números complexos  $\mathbb{C}$  e seus subcorpos, entre os quais, o corpo dos números racionais  $\mathbb{Q}$ .
- O corpo dos números algébricos.
- O corpo dos números reais  $\mathbb{R}$ .
- $\mathbb{Z}_2$ , é o menor corpo finito, formado pelos números 1 e 0, em que  $1 + 1 = 0$ . Este conjunto com as operações de adição e multiplicação satisfaz todos os axiomas de um *anel*, é *comutativo* e tem *unidade* (elemento neutro). Além disso, como em qualquer anel com unidade, 1 é o elemento inverso de 1.

- $\mathbb{Z}_p$ , onde  $p$  é um número primo é um corpo finito com elementos:  
 $\mathbb{Z}_p = \{0, 1, 2, \dots, p - 1\}$ .
- O menor e mais básico corpo numérico infinito é o corpo  $\mathbb{Q}$  dos números racionais. Muitas propriedades dos corpos numéricos gerais, tais como a fatoração única, são modeladas com base nas propriedades de  $\mathbb{Q}$ .

**Contra-exemplo:**  $\mathbb{Z}_n$ , quando  $n$  não é um número primo, não é um corpo, pois tem divisores de zero.

## 6.9 Conceituando um Espaço matemático

Um *espaço matemático* é uma estrutura algébrica similar à de um conjunto, porém dotada de alguma estrutura matemática adicional.

## 6.10 Conceituando um Espaço Métrico

Definida uma *métrica*, podemos agora explicar o que vem a ser um *espaço métrico*. Um conjunto em que há uma *métrica* definida recebe o nome de *espaço métrico*.

Em Matemática, um *espaço métrico* é um conjunto onde as *distâncias entre quaisquer de seus elementos* é definida. Estas distâncias são dadas pela *métrica* definida no conjunto.

O *espaço métrico* mais familiar é o *espaço euclidiano*. A *métrica euclidiana* define a distância entre dois pontos como o comprimento do segmento de reta que os conecta. Na verdade, a *métrica* é uma generalização das quatro propriedades conhecidas da *distância euclidiana*.

Existem outros espaços métricos, por exemplo na *geometria elíptica*. Mesmo no *espaço euclidiano*, podemos adotar uma medida diferente de *distância*, como a *métrica de Manhattan*, como mostrado na Figura 95:

Na Figura 95, a Métrica de Manhattan, pode ser vista com a linha em vermelho, com a linha em amarelo, e com a linha em azul. São todas caminhos que tem o comprimento mais curto entre os pontos de início e fim dos caminhos. Na geometria euclidiana, a linha verde tem o comprimento  $6\sqrt{2} \approx 8.496\sqrt{2} \approx 8.49$ , e é o único caminho mais curto.

A partir daí, podemos definir *propriedades topológicas* como *conjuntos abertos* e *conjuntos fechados*, que levam ao estudo de *espaços topológicos* mais abstratos.

### Definição (Espaços Métricos)

Seja  $X$  um conjunto qualquer. Uma métrica definida sobre  $X$  é uma função  $d : X \times X \rightarrow R$  que satisfaz as seguintes propriedades:

1.  $d(x, y) \geq 0 \quad \forall x, y \in X$  e  $d(x, y) = 0 \Leftrightarrow x = y$ ;
2.  $d(x, y) = d(y, x) \quad \forall x, y \in X$ ;

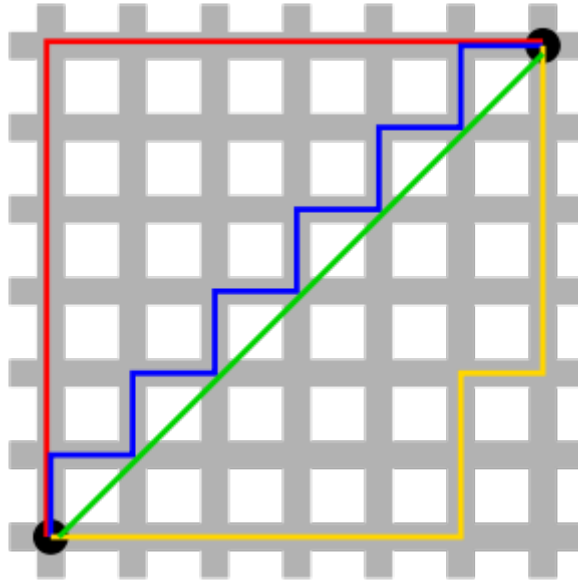


Figura 95 – Métrica de Manhattan versus Distância Euclidiana.

Fonte: <[https://en.wikipedia.org/wiki/Taxicab\\_geometry](https://en.wikipedia.org/wiki/Taxicab_geometry)>

3.  $d(x, z) \leq d(x, y) + d(y, z) \quad \forall x, y, z \in X$ ,  
(essa propriedade é conhecida como *desigualdade triangular*).

Então o par  $(X, d)$  é chamado um *espaço métrico*.

Ignorando o rigor matemático, para qualquer sistema de estradas e terrenos a distância entre duas localidades pode ser definida como o comprimento da rota mais curta que liga esses locais. Para ser uma *métrica*, não deve haver estradas de mão única. A desigualdade triangular expressa o fato de que os desvios não são atalhos.

## 6.11 O conceito de Espaço Vetorial

Um dos conceitos básicos em Álgebra Linear é o espaço vetorial. A noção comum de *vetores* como objetos com *tamanho*, *direção* e *sentido*, juntamente com as operações de adição de vetores e multiplicação de vetores por números reais, formam a ideia básica de um espaço vetorial. Deste ponto de partida então, para definirmos um espaço vetorial, precisamos de um *conjunto*, uma *operação de adição de elementos deste conjunto*, e uma *operação de multiplicação de escalares* (por exemplo, números reais) por elementos deste conjunto. *Polinômios* de grau menor ou igual a  $n$  ( $n \in \mathbb{N}$ ) formam um espaço vetorial, por exemplo; assim como os grupos de matrizes  $m \times n$  e o espaço de todas as funções de um conjunto no conjunto  $\mathbb{R}$  dos números reais.

Na geometria euclidiana e na mecânica clássica, o *espaço euclidiano tridimensional* é um espaço vetorial definido como o conjunto de posições que possa ser descrito atribuindo-se a cada posição três coordenadas, respeitadas duas condições: (a) validade do teorema de Pitágoras, e (b) respeito à norma euclidiana.

Um *espaço vetorial* é usado para representar um universo de *vetores*.

Não é necessário que os vetores tenham interpretação geométrica, mas podem ser quaisquer objetos que satisfaçam os axiomas seguintes.

**Definição** (Espaço Vetorial)

Um *espaço vetorial*  $\mathcal{S}$ , com um conjunto  $\mathcal{H}$  sobre  $\mathcal{K}$ , é uma *álgebra*

$$\mathcal{S} = (\mathcal{H}, +, ^{-1}, 0, K, +_f, \times_f, 0, 1, \cdot)$$

tal que  $(\mathcal{H}, +, ^{-1}, 0)$  é um grupo comutativo,  $\mathcal{K} = (K, +_f, \times_f, 0, 1)$  é um corpo, e  $\cdot : K \times \mathcal{H} \rightarrow \mathcal{H}$  é uma *multiplicação escalar* satisfazendo os seguintes axiomas para quaisquer  $a, b \in K$  e quaisquer  $\phi, \psi \in \mathcal{H}$ :

- $a \cdot (\phi + \psi) = a \cdot \phi + a \cdot \psi$  e  $(a +_f b) \cdot \phi = a \cdot \phi + b \cdot \psi$
- $(a \cdot (b \cdot \phi)) = (a \times_f b) \cdot \phi$
- $1 \cdot \phi = \phi$

Feita esta definição, a partir de agora não faremos mais distinção entre os operadores  $+$ ,  $+_f$  e  $\times_f$ , exceto quando necessário. Além disso, escreveremos  $(\phi - \psi)$  no lugar de  $(\phi + \psi^{-1})$ .

## 6.12 Norma matemática

Em matemática, uma *norma* consiste em uma função que a cada vetor de um espaço vetorial associa um número real não-negativo. O conceito de norma está intuitivamente relacionado à noção geométrica de *comprimento*.

**Definição** (Norma)

Dado um espaço vetorial  $X$  sobre um corpo  $\mathbb{K}$  dos números reais ou complexos, uma função  $\|\cdot\| : X \rightarrow \mathbb{R}^+$  é chamada de *norma* se, para quaisquer  $x, y \in X$  e todo  $\alpha \in \mathbb{K}$ :

- $\|x\| = 0 \Rightarrow x = 0$ . Se esta condição não for atendida, a função será no máximo uma *seminorma*.
- $\|\alpha x\| = |\alpha| \|x\|$ .
- $\|x + y\| \leq \|x\| + \|y\|$  (é a chamada *desigualdade triangular*).

**Definição** (Espaço Vetorial Normado)

Se o espaço vetorial  $X$  tem uma *norma*, ele passa a ser chamado de *espaço vetorial normado*, e denotado por  $(X, \|\cdot\|)$ .

### 6.13 Métrica e topologia induzida

Toda *norma* induz, de forma natural, uma *métrica*  $d$  em  $X$ , cujos valores são dados por:

$$d(x, y) = \|x - y\|.$$

Em Matemática, uma *métrica* é um conceito que generaliza a noção geométrica de *distância*.

O conceito de *norma* também induz o que vem a ser uma *topologia*  $\tau$  que será definida *a posteriori*.

### 6.14 Conceituando um Espaço Topológico

No campo da Matemática, a *forma canônica* refere-se de forma geral à *forma normal e clássica* de representar uma dada relação.

Por exemplo, no *espaço euclidiano*  $\mathbb{R}^3$ , o *produto interno canônico* de vetores  $u = (u_1, u_2, u_3)$  e  $v = (v_1, v_2, v_3)$  é definido assim:

$$\langle u | v \rangle = u_1 \cdot v_1 + u_2 \cdot v_2 + u_3 \cdot v_3 = \sum p_i = \sum (u_i \cdot v_i) \quad (6.1)$$

Outro exemplo é pensar em espaços vetoriais, utilizando a base canônica de geração de vetores, como no caso do espaço vetorial euclidiano  $\mathbb{R}^2$ , cuja base canônica  $\{b_1, b_2\}$  é dada pelos vetores  $b_1 = (x, y) = (1, 0)$  e  $b_2 = (x, y) = (0, 1)$

A todo *espaço métrico* está associado, de *forma canônica*, um *espaço topológico*. Esse *espaço topológico* pode ser definido de várias maneiras equivalentes. Adotaremos a definição seguinte:

*Espaços topológicos* são estruturas que permitem a formalização de conceitos tais como *convergência*, *conexidade* e *continuidade*. Eles aparecem em praticamente todos os ramos da matemática moderna e são, hoje, uma noção unificadora central. O ramo da Matemática que estuda os *espaços topológicos* é denominado *Topologia*. É ensinada como uma disciplina de graduação a alunos dos cursos de bacharelado em Matemática.

#### Definição (Espaço Topológico)

Uma *topologia* em um conjunto  $X$  é uma coleção  $\tau$  de partes de  $X$ , chamados os *conjuntos abertos* da topologia  $\tau$ , com as seguintes propriedades:

1.  $X \in \tau$ ;
2. Se  $A_1, A_2 \in \tau$ , então  $A_1 \cap A_2 \in \tau$ ;
3. Dada uma família arbitrária  $(A_\lambda)_{\lambda \in L}$ , com  $A_\lambda \in \tau$ ,  $\forall \lambda \in L$  tem-se  $(\bigcup_{\lambda \in L} A_\lambda) \in \tau$ .

Um espaço topológico é um par  $(X, \tau)$ , onde  $X$  é um conjunto e  $\tau$  é uma topologia em  $X$ .

### Exemplos de Topologias

- Se  $X$  é um conjunto, a topologia  $\tau = P(X)$ , onde  $P(X)$  é o conjunto das partes de  $X$  é denominada a *topologia discreta* sobre  $X$ .
- Se  $X$  é um conjunto, a topologia  $\tau = \{\emptyset, X\}$  é denominada a topologia grosseira sobre  $X$ .
- Um espaço métrico  $(X, d)$  tem uma estrutura natural de espaço topológico para  $\tau$  definido como o conjunto das uniões de bolas abertas  $B(x, \delta)$  tal que  $B(x, \delta) = \{y \in X : d(x, y) < \delta\}$ .
- Nada impede que, a um conjunto  $X$ , esteja associada a mais de uma *topologia*, por exemplo,  $\tau_1$  e  $\tau_2$ . Quando todo conjunto aberto de  $\tau_1$  for um aberto de  $\tau_2$ , diz-se que a *topologia*  $\tau_1$  é mais grossa que  $\tau_2$ , ou, analogamente, que  $\tau_2$  é mais fina que  $\tau_1$ . Como o próprio nome indica, a topologia “grosseira” é mais grossa que qualquer outra, e a topologia discreta é mais fina que qualquer outra.

## 6.15 Produto interno

Em matemática, chamamos de *produto interno* em um espaço vetorial, uma função de dois vetores que satisfaz determinados axiomas. O *produto escalar*, comumente usado na *geometria euclidiana*, é um caso especial de *produto interno*.

Também em matemática, o *produto vetorial*, é uma operação binária sobre vetores em um espaço vetorial. Seu resultado difere do produto interno (que tem como resultado um *escalar*, um *número*) por ser também um *vetor*, ao invés de um escalar (número). Seu principal uso baseia-se no fato que o resultado de um produto vetorial é sempre *perpendicular* a ambos os vetores originais.

### Definição - (Produto Interno)

Seja  $X$  um espaço vetorial sobre um corpo ( $\mathbb{R}$  ou  $\mathbb{C}$ ). Um *produto interno* sobre  $X$  é uma função  $\langle \cdot | \cdot \rangle : X \times X \rightarrow \mathbb{K}$  que associa a cada par ordenado de vetores  $x, y \in X$  um escalar  $\langle x | y \rangle$  chamado o produto interno de  $x$  por  $y$ , de modo que sejam satisfeitas as seguintes condições para quaisquer  $x, y, z \in X, \lambda \in \mathbb{K}$ :

- $\langle \lambda(x + y) | z \rangle = \lambda \langle x | z \rangle + \lambda \langle y | z \rangle$
- $\langle x | x \rangle \geq 0$
- $\langle x | x \rangle = 0 \Rightarrow x = 0$
- $\langle x | y \rangle = \langle y | x \rangle$



$$\bullet \langle x | \lambda(y + z) \rangle = \lambda \langle x | y \rangle + \lambda \langle x | z \rangle$$

## 6.16 Norma a partir de um produto interno

Seja  $X$  um espaço vetorial munido de um produto interno  $\langle \cdot | \cdot \rangle$ . A partir de  $\langle \cdot | \cdot \rangle$  construiremos uma função  $\|\cdot\| : X \rightarrow \mathbb{R}$ , pondo  $\|x\| = (\langle x, x \rangle)^{1/2}$ ,  $\forall x \in X$ .

A seguir, um importante resultado referente à função construída acima:

**Teorema** (Desigualdade de Cauchy-Bunyakowsky-Schwarz) (CBS)

$$|\langle x, y \rangle| \leq \|x\| \cdot \|y\|, \forall x, y \in X$$

A função  $\|\cdot\| : X \rightarrow \mathbb{R}$  acima construída, a partir do produto interno  $\langle \cdot | \cdot \rangle$  é uma norma em  $X$ . Neste caso, dizemos que a norma  $\|\cdot\|$  provém do produto interno  $\langle \cdot | \cdot \rangle$ .

### Exemplo

A) A norma euclidiana  $|\cdot| : \mathbb{C} \rightarrow \mathbb{R}$  (função módulo) dada por  $|a| = \sqrt{a_1^2 + a_2^2}$ ,  $\forall a, a = a_1 + i.a_2 \in \mathbb{C}$ , provém do produto interno  $\langle \cdot | \cdot \rangle$  dado por  $\langle a_1 + i.a_2 | b_1 + i.b_2 \rangle = a_1.b_1 + a_2.b_2 \forall a = a_1 + i.a_2, b = b_1 + i.b_2 \in \mathbb{C}$

## 6.17 Espaços completos

Em Matemática, uma **sucessão** ou **sequência** de Cauchy ou sequência de Cauchy é uma sucessão tal que a distância entre os termos vai se aproximando de zero. Deve o seu nome ao matemático francês **Augustin Louis Cauchy** (1789-1857). Intuitivamente é uma sequência onde seus termos vão ficando cada vez mais próximos.

**Definição** - (Sucessão de Cauchy para números reais)

Uma sequência  $(x_n)$ ,  $n \in \mathbb{N}$  é chamada de *sequência de Cauchy*, se para qualquer número positivo  $\epsilon$ ,  $\exists n \in \mathbb{N}$ ,  $n_0$ , tal que se  $n, m$  são maiores do que  $n_0$ , a distância entre  $x_n$  e  $x_m$  é menor do que  $\epsilon$ .

Em linguagem simbólica temos:

$$\forall \epsilon > 0, \exists n_0 \in \mathbb{N} : n, m \geq n_0, |x_n - x_m| < \epsilon.$$

Nos reais  $\mathbb{R}$ , uma sequência é convergente se, e somente se, for de Cauchy: esta propriedade é chamada de *completude* e torna os números reais  $\mathbb{R}$  um espaço completo.

**Definição** - (Espaços métricos)

Estendendo a definição para espaços métricos quaisquer, temos:

Se  $M$  é um espaço métrico e  $d : M \times M \rightarrow \mathbb{R}$  sua métrica, dizemos que  $(x_n)_{n \in \mathbb{N}} \subset M$  diz-se que:



Figura 96 – Augustin Cauchy - Matemático francês que se destacou no estudo das sequências e séries numéricas no século XVIII.

Fonte: <[https://pt.wikipedia.org/wiki/Augustin-Louis\\_Cauchy](https://pt.wikipedia.org/wiki/Augustin-Louis_Cauchy)>

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \mid n, m \geq n_0 \Rightarrow d(x_n, x_m) < \epsilon$$

Em espaços normados, esta definição se escreve como:

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \mid n, m \geq n_0 \Rightarrow |x_n - x_m| < \epsilon$$

### Exemplos (Sequência de Cauchy)

$(x_n)_{n \in \mathbb{N}^*}$  em  $\mathbb{R}$ , dada por  $x_n = 1/n$ ,  $\forall n \in \mathbb{N}$ .

De fato, dado  $\epsilon > 0$ , pela propriedade arquimediana, podemos encontrar  $n_0$ , tal que  $1/n_0 < \epsilon$ , então se  $n, m \geq n_0$ , sem perda de generalidade, podemos supor que  $n \geq m$ , assim, teremos  $0 < 1/n \leq 1/m \leq 1/n_0$ . De onde concluímos que:

$$|1/n - 1/m| \leq |1/n_0 - 0| = 1/n_0 < \epsilon$$

e portanto  $(x_n)$  é uma sequência de Cauchy.

### Definição - Convergência e espaço completo

Qualquer sucessão convergente (no sentido usual) é de **Cauchy**, no entanto existem espaços contendo sucessões de **Cauchy** não convergentes. Por exemplo, a sucessão  $(1/n)$  é de Cauchy, mas não é convergente no intervalo  $(0, 1)$  (embora o seja em  $\mathbb{R}$ ). Um espaço onde todas as sucessões de **Cauchy** são convergentes chama-se um *espaço completo*.

Dado  $E$  um **espaço métrico** qualquer, é possível construir uma extensão de  $E$  que é um **espaço métrico completo**. Esta extensão é única (no sentido categorial), ou seja, dadas duas completudes de  $E$  elas são isométricas.

Um espaço métrico é **completo** quando todas as sequências de Cauchy convergem para um limite que pertence ao espaço.

**Exemplos** - (Espaços Completos)

O conjunto dos números reais  $\mathbb{R}$  com a métrica usual  $d(x, y) = |x - y|$  é completo.

Qualquer subconjunto fechado de  $\mathbb{R}$  é completo.

## 6.18 Bibliografia e Fonte de Consulta

Jacy Monteiro (1969) - Álgebra Abstrata - IMPA, Rio de Janeiro.

Michel Spivak (2011) - Calculus, vol I e II, 1970.

Lam, Tsit-Yuen (2001), A First Course in Noncommutative Rings, Berlin, New York: Springer-Verlag, ISBN 978-0-387-95325-0.

Lang, Serge (2002), Algebra, Graduate Texts in Mathematics, 211 (Revised third ed.), New York: Springer-Verlag, MR1878556, ISBN 978-0-387-95385-4.

Rudin, Walter. Principles of Mathematical Analysis. Col: Walter Rudin Student Series in Advanced Mathematics 3rd ed. [S.l.]: McGraw-Hill. ISBN 978-0-07-054235-8.

Abbott, Stephen (2001). Understanding Analysis. Col: Undergraduate Texts in Mathematics. New York: Springer-Verlag. ISBN 0-387-95060-5

## 6.19 Para saber mais - Leitura Recomendada

Augustin Louis Cauchy - <[https://pt.wikipedia.org/wiki/Augustin\\_Louis\\_Cauchy](https://pt.wikipedia.org/wiki/Augustin_Louis_Cauchy)>

## Espaços de Hilbert

Por volta de 300 a.C., o matemático grego **Euclides** estabeleceu as leis do que veio a ser chamado "Geometria Euclidiana", que é o estudo das relações entre ângulos e distâncias num espaço de dimensão finita. Um **espaço euclidiano** é um espaço vetorial real (em  $\mathbb{R}$ ) de dimensão finita munido de um *produto interno*.

$$\begin{aligned} \mathbf{e}_1 &= (1, 0, \dots, 0), \\ \mathbf{e}_2 &= (0, 1, \dots, 0), \\ &\vdots \\ \mathbf{e}_n &= (0, 0, \dots, 1). \end{aligned}$$

Figura 97 – O espaço vetorial  $\mathbb{R}^n$  vem com uma base padrão (base canônica).

Um vetor arbitrário em  $\mathbb{R}^n$  pode então ser escrito na forma:

$$x = \langle e \mid x \rangle = \sum_{n=1}^n e_i \cdot x_i$$

$\mathbb{R}^n$  é o exemplo perfeito de um espaço vetorial real  $n$ ,  $n$ -dimensional. Todo espaço vetorial real  $n$ -dimensional  $V$  é isomórfico a  $\mathbb{R}^n$ . Entretanto, esse isomorfismo não é *canônico*. Uma escolha de isomorfismo é equivalente a uma escolha da base para  $V$  (olhando a imagem da base padrão para  $\mathbb{R}^n$  em  $V$ ). A razão para se trabalhar com espaços vetoriais arbitrários em vez de  $\mathbb{R}^n$  é que, geralmente, é preferível trabalhar de uma maneira independente de coordenadas (isto é, sem escolher uma base preferida).

### 7.1 Espaços de Hilbert

**Definição** - Na matemática, um espaço de **Hilbert** é uma generalização do **espaço euclidiano** que não precisa estar restrita a um número finito de dimensões.

É um espaço vetorial dotado de produto interno, ou seja, com noções de distância e ângulos. Esse espaço obedece uma relação de completude, que garante que os limites

existem quando esperados, o que permite e facilita diversas definições da Análise.

Os espaços de **Hilbert** permitem que, de certa maneira, noções intuitivas sejam aplicadas em *espaços funcionais*. Por exemplo, com eles podemos generalizar os conceitos de *séries de Fourier* em termos de polinômios ortogonais. Os espaços de **Hilbert** são de importância crucial para a mecânica quântica.



Figura 98 – David Hilbert - Criação dos espaços que levam seu nome, durante seus trabalhos em análise sobre equações integrais.

Fonte: <[https://pt.wikipedia.org/wiki/David\\_Hilbert](https://pt.wikipedia.org/wiki/David_Hilbert)>

Espaços de **Hilbert** foram criados por **David Hilbert**, que os estudou no contexto de equações integrais. **John von Neumann** criou a nomenclatura "*der abstrakte Hilbertsche Raum*" em seu famoso trabalho em *operadores Hermitianos não limitados* publicado em 1929. Talvez, **John Von Neumann** seja o matemático que melhor reconheceu a importância desse trabalho original.

Os elementos de espaço de **Hilbert** abstrato são chamados vetores. Em aplicações, eles são tipicamente sequências de números complexos ou funções. Na *mecânica quântica*, por exemplo, **um sistema físico é descrito por um espaço de Hilbert complexo** que contém os **vetores de estado**, que contém todas as informações do sistema com suas complexidades.

Os espaços de **Hilbert** fornecem o formalismo apropriado para o estudo de conceitos da *mecânica quântica* e, portanto, da *computação quântica*. Neste capítulo definimos espaços de **Hilbert**, estabelecemos nossas notações e listamos algumas propriedades importantes.

## 7.2 Base Canônica

**Definição** (Base Canônica)

Na matemática, a *base canônica* de um espaço vetorial (uma álgebra vetorial) ou de

outras estruturas algébricas semelhantes é a base mais primitiva (base geradora) e intuitiva para a estrutura.

Por exemplo:

- No  $\mathbb{R}^2$ , a base canônica é dada pelo conjunto  $\{(1, 0), (0, 1)\}$ .
- Analogamente, no  $\mathbb{R}^n$ , a base canônica é formada pelos vetores que tem 1 em uma coordenada e 0 nas demais (CALLIOLI; DOMINGUES; COSTA, 1990).
- De modo ainda mais genérico, no espaço vetorial  $\mathcal{K}^n$  para um corpo  $\mathbb{K}$  qualquer, a base canônica é o conjunto de  $n$  vetores  $v_i$ , em que cada vetor  $v_i$  tem a  $i$ -ésima coordenada igual a  $\delta_{ij}$ , sendo  $\delta$  a *função delta* de **Kronecker**. Na matemática, o  $\delta$  de **Kronecker**, assim chamado em honra a **Leopold Kronecker** (1823-1891), é a notação  $\delta_{ij}$  definida por:

$$\delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$



Figura 99 – Leopold Kronecker - Uma das suas frases mais famosas é: Deus criou os inteiros; todo o resto é trabalho do homem.

Fonte: <[https://pt.wikipedia.org/wiki/Leopold\\_Kronecker](https://pt.wikipedia.org/wiki/Leopold_Kronecker)>

Note-se que, a rigor, o  $\delta$  de **Kronecker** não é uma função, pois ele pode ser usado com qualquer símbolo matemático. Seu uso mais comum é como função de domínio  $\mathbb{Z} \times \mathbb{Z}$  mas pode ter outras restrições de domínios ou outros conjuntos mais gerais.

**Leopold Kronecker** foi um matemático alemão. **Kronecker** estudou em Berlim e obteve o grau de doutor em 1845, com uma tese sobre Teoria dos Números. Suas principais contribuições para a matemática foram no campo da álgebra e continuidade de funções.

- Na álgebra  $K[x]$  dos polinômios com coeficientes no corpo  $K$ , a base canônica é o conjunto enumerável  $\{1, x, x^2, \dots\}$ .
- Se um corpo  $E$  é uma extensão finita simples do corpo  $F$  a partir do elemento  $\alpha$  (ou seja,  $E = F[\alpha]$ ), a base canônica de  $E$  (como espaço vetorial de  $F$ ) é o conjunto de  $n$  elementos  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ , em que  $n$  é o grau de  $\alpha$  em  $F$ .

### 7.3 Espaço vetorial com produto interno

**Definição** (Produto interno)

Um espaço com *produto interno complexo*  $\mathcal{H}$  é um espaço vetorial com um conjunto  $\mathcal{H}$  sobre o corpo dos números complexos, munido de um *produto interno*  $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$  satisfazendo os seguintes axiomas. Para quaisquer  $\phi, \phi', \psi \in \mathcal{H}$  e quaisquer  $a, b \in \mathbb{C}$ :

- $\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^*$
- $\langle \psi | \psi \rangle \geq 0$ , com  $\langle \psi | \psi \rangle = 0$  se, e somente se,  $\psi = 0$ .
- $\langle \psi | a\phi + b\phi' \rangle = a \langle \psi | \phi \rangle + b \langle \psi | \phi' \rangle$

### 7.4 Espaço vetorial, Produto interno e Norma

**Definição** (Norma)

Sejam  $\mathcal{S}$  um espaço vetorial com produto interno complexo  $\mathbb{C}$  e  $\phi, \psi \in \mathcal{S}$ . A *norma* de  $\phi$  é definida por  $\|\phi\| := \sqrt{\langle \phi | \phi \rangle}$ . A distância entre os vetores  $\phi$  e  $\psi$  é dada por  $dist(\phi, \psi) := \|\phi - \psi\|$ .

Se tivermos  $\mathcal{H} = \mathbb{C}^n$  e o produto interno definido como

$$\langle (x_1, \dots, x_n) | (y_1, \dots, y_n) \rangle = \sum_{i=1}^n x_i^* y_i, \text{ então falamos sobre o espaço vetorial com produto interno complexo } n\text{-dimensional.}$$

Considere um espaço com produto interno complexo  $\mathcal{H}$ . Para quaisquer vetores  $\phi, \psi \in \mathcal{H}$  e qualquer  $c \in \mathbb{C}$ , valem as seguintes propriedades:

- (a)  $\langle c\phi | \psi \rangle = c^* \langle \phi | \psi \rangle$
- (b)  $\|c\phi\| = |c| \|\phi\|$
- (c)  $|\langle \phi | \psi \rangle| \leq \|\phi\| \|\psi\|$  (desigualdade de Cauchy-Schwarz)
- (d)  $\|\phi + \psi\| \leq \|\phi\| + \|\psi\|$  (desigualdade triangular)
- (e)  $\|\phi + \psi\|^2 + \|\phi - \psi\|^2 = 2\|\phi\|^2 + 2\|\psi\|^2$  (lei do paralelogramo)

A demonstração destas propriedades estão no Apêndice A em (CARDONHA; SILVA; FERNANDES, 2004).

## 7.5 Definições do Espaço de Hilbert

### Definição 1 (Espaço de Hilbert)

Um espaço de **Hilbert** é um **espaço vetorial com produto interno** que também é um espaço de **Banach** com a norma canônica definida pelo produto interno:

$$\|x\| = \sqrt{\langle x | x \rangle}.$$

### Definição 2 (Espaço de Hilbert)

Um espaço de **Hilbert**  $\mathcal{H}$  é um **espaço vetorial normado**, dotado de produto interno  $\langle \cdot, \cdot \rangle$ , tal que  $\mathcal{H}$  é completo quando munido com a métrica  $d(u, v) = \|u - v\| = \sqrt{\langle u - v | u - v \rangle}$ , onde  $\|\cdot\|$  é a norma que provém do produto interno  $\langle \cdot | \cdot \rangle$ .

Os elementos de um espaço de **Hilbert** abstrato são chamados *vetores*. Em aplicações, esses espaços são tipicamente *sequências de funções*.

### Exemplos

(a) O espaço  $\mathbb{C}$ , munido do produto interno  $\langle a_1 + i.a_2, b_1 + i.b_2 \rangle = a_1.b_1 + a_2.b_2$ , onde  $i = \sqrt{-1}$ , é um espaço de Hilbert.

(b) O espaço  $\mathcal{L}^2$ , munido do produto interno  $\langle (x_n) | (y_n) \rangle = \sum_{i=1}^{\infty} x_i.\overline{y_i}$ , é um espaço de **Hilbert**.

### Definição (Sequência infinita em $\mathcal{H}$ convergente)

Dada uma sequência infinita  $\phi_1, \phi_2, \dots, \phi_n \in \mathcal{H}$ , onde  $\mathcal{H}$  é um espaço com produto interno complexo, dizemos que ela *converge* para  $\phi \in \mathcal{H}$  se, para qualquer  $\epsilon > 0$ , existir um número  $N(\epsilon)$  tal que  $\|\phi_i - \phi\| < \epsilon$ , para todo  $i > N(\epsilon)$ .

Além disso, tal sequência infinita é chamada de sequência de Cauchy se, para qualquer  $\epsilon > 0$ , existir um número  $M(\epsilon)$  tal que  $\|\phi_i - \phi_j\| < \epsilon$  para quaisquer  $i, j > M(\epsilon)$ .

Se toda sequência de Cauchy em  $\mathcal{H}$  converge, dizemos que  $\mathcal{H}$  é *completo*.

### Definição 3 (Espaço de Hilbert)

Um espaço de **Hilbert** é um espaço vetorial  $\mathcal{H}$  sobre o corpo dos complexos  $\mathbb{C}$  e dotado de um produto interno, tal que dados os vetores  $u, v \in \mathcal{H} \mapsto \langle u.v \rangle \in \mathbb{C}$ .  $\mathcal{H}$  é dito ser um **Espaço de Hilbert**, se for *completo* em relação à métrica  $d$  definida por esse produto interno:

$$d(u, v) = \|u - v\| = \sqrt{\langle u - v, u - v \rangle}, \text{ onde } u, v \in \mathcal{H}.$$

### Definição 4 (Espaço de Hilbert)

Um espaço de **Hilbert** é um espaço *completo* com *produto interno* complexo  $\mathbb{C}$ .



## Espaço de Banach

Em matemática, um espaço de **Banach** é um **espaço vetorial normado completo**. Deve seu nome ao matemático a **Stefan Banach** (1892-1945), um matemático polonês. Sua principal contribuição foi a moderna *Análise Funcional* (espaços de funções).

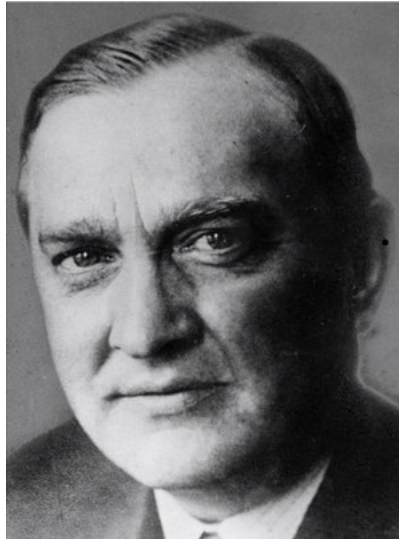


Figura 100 – Stefan Banach - o criador da moderna Análise Funcional, que trata do estudo de espaços de funções.

Fonte: <[https://pt.wikipedia.org/wiki/Stefan\\_Banach](https://pt.wikipedia.org/wiki/Stefan_Banach)>

Um grande impulso para o avanço da *análise funcional* durante o século XX foi a modelagem, devida a **John von Neumann** (1903-1957), da **mecânica quântica em espaços de Hilbert**.

A *Análise Funcional* é o ramo da matemática, e mais especificamente da *análise matemática*, que trata do estudo de *espaços de funções*. Tem suas raízes históricas no estudo de *transformações*, tais como a *Transformada de Fourier*, e no estudo de *equações diferenciais* e *equações integrais*. A palavra *funcional* remonta ao **Cálculo de Variações**, implicando uma função cujo argumento é uma função. Seu uso em geral é atribuído ao matemático italiano **Vito Volterra** (1860-1940). Seu trabalho mais relevante é relacionado a *equações integrais*. Publicou em 1896 artigos sobre o tema, conhecido como Equações Integrais de **Volterra**.

Os números reais e os números complexos são espaços de **Banach** onde a norma  $\|..\|$  é o próprio valor absoluto  $|..|$ .

Exemplos:

- Qualquer espaço de **Hilbert** é um espaço de **Banach**.
- O espaço das funções contínuas reais definidas no intervalo  $[0, 1]$ , é um espaço de **Banach** com a *norma* do supremo:

$$\|f\| = \sup_{x \in [0,1]} |f(x)|$$

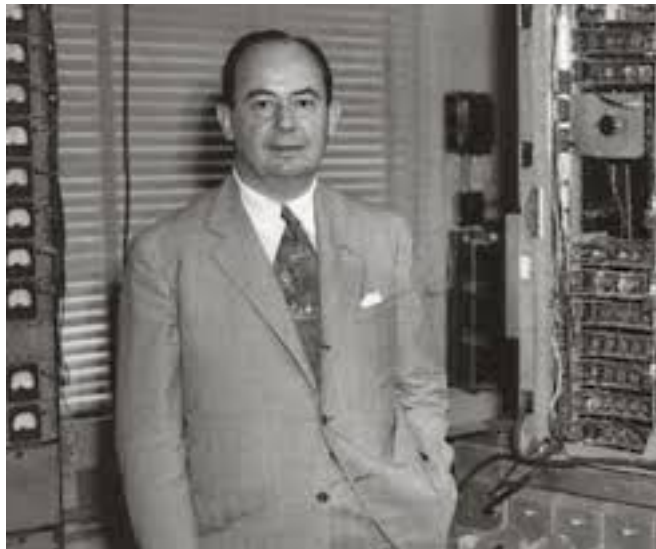


Figura 101 – John von Neumann - Modelou a mecânica quântica em um espaço de Hilbert.

Fonte: <[https://pt.wikipedia.org/wiki/John\\_von\\_Neumann](https://pt.wikipedia.org/wiki/John_von_Neumann)>



Figura 102 – Volterra - Quem criou a palavra "funcional" no Cálculo das Variações.

Fonte: <[https://pt.wikipedia.org/wiki/Vito\\_Volterra](https://pt.wikipedia.org/wiki/Vito_Volterra)>

Toda *função contínua* é limitada num *conjunto compacto*, portanto a *norma* está bem definida. Os axiomas da *norma* são facilmente verificados. Ainda, convergência nesta *norma* é equivalente à *convergência uniforme*. Como *convergência uniforme*

preserva continuidade, o espaço é *completo*.

**Álgebra de Banach** - É quando o espaço é uma *álgebra sobre um corpo*, com propriedades consistentes entre o *produto de vetores* e a *norma*.

## 7.6 Espaço de Hilbert conjugado

**Definição** (função linear)

Uma função  $f : \mathcal{H} \rightarrow \mathbb{C}$  é dita linear se  $f(a\phi + b\psi) = af(\phi) + bf(\psi)$ , para quaisquer  $\phi, \psi \in \mathcal{H}$  e quaisquer  $a, b \in \mathbb{C}$ . Dizemos também que  $f$  é um *funcional*.

É possível provar que para todo funcional  $f$ , existe um único  $\phi_f \in \mathcal{H}$  tal que  $f(\psi) = \langle \phi_f | \psi \rangle$ , para todo  $\psi \in \mathcal{H}$ .

O conjunto de todos os funcionais de um espaço de Hilbert  $\mathcal{H}$  é também um espaço de Hilbert (se definirmos a adição e a multiplicação da maneira usual). Tal espaço é denominado *dual do espaço de Hilbert*  $\mathcal{H}$  ou *espaço de Hilbert conjugado*, denotado por  $\mathcal{H}^*$ , com produto interno  $\langle f | g \rangle = \langle \phi_f | \phi_g \rangle$ , para todo  $f, g \in \mathcal{H}^*$ .

Desta forma, estabelece-se uma bijeção entre  $\mathcal{H}$  e  $\mathcal{H}^*$ , e portanto todo espaço de Hilbert é *isomorfo* (existe um isomorfismo) ao seu dual.

Dado um elemento  $\phi \in \mathcal{H}$  como um vetor na notação de **Dirac** (DIRAC, 1939), temos que para qualquer  $\psi \in \mathcal{H}$ , temos  $\langle \phi | \psi \rangle$  representando o produto externo.

Se estivermos falando de um *espaço de Hilbert n-dimensional* podemos pensar em  $|\phi\rangle$  como um vetor coluna de dimensão  $n$  e  $\langle\psi|$  como um vetor linha de mesma dimensão. Neste caso, a transformação

$$|\phi\rangle\langle\psi|$$

Figura 103 – Em um espaço de Hilbert n-dimensional, como podemos ver o produto externo de estados.

Fonte: (CARDONHA; SILVA; FERNANDES, 2004)

corresponde a uma *transposição* e uma *conjugação*. O **produto externo**  $|\phi\rangle\langle\psi|$  equivale, portanto, a uma matriz de dimensão  $n$ , utilizando-se a definição usual de multiplicação de matrizes. O mesmo se aplica ao cálculo do **produto interno**.

## 7.7 Ortogonalidade e Ortonormalidade

A *ortogonalidade* é um conceito de extrema importância para a computação quântica. Numa medição, só é possível distinguir estados quânticos mutuamente ortogonais.

**Definição** (Vetores Ortogonais)

Dois vetores não-nulos  $\phi, \psi \in \mathcal{H}$  são ortogonais, o que se denota por  $\phi \perp \psi$ , se

$\langle \phi | \psi \rangle = 0$ . Um conjunto  $\mathcal{S} \subseteq \mathcal{H}$  é ortogonal se cada par de elementos distintos do conjunto forem ortogonais.

**Definição** (Vetores Ortonormais)

Um conjunto ortogonal é chamado *ortonormal* se todos seus elementos têm norma 1.

**Proposição** Seja  $\mathcal{B} \subseteq \mathcal{H}$  um conjunto ortogonal com  $n$  elementos. Então os vetores de  $\mathcal{B}$  são *linearmente independentes*.

A demonstração está na seção A.3, no Apêndice A em (CARDONHA; SILVA; FERNANDES, 2004).

**Definição** (Base Ortonormal)

Um conjunto ortonormal  $\mathcal{B} \in \mathcal{H}$  é uma *base ortonormal* de  $\mathcal{H}$ , se todo vetor  $v \in \mathcal{H}$  pode ser escrito como:  $v = \sum_{\phi \in \mathcal{B}} a_{\phi} \phi$ , com  $a_{\phi} \in \mathbb{C}$ , para todo  $\phi \in \mathcal{B}$ .

**Definição** (Combinação Linear dos elementos de uma base  $\mathcal{B}$ )

Seja  $\mathcal{B} = \{\phi_i\}_{i=1}^n$  uma base para um espaço de Hilbert  $\mathcal{H}$  e  $\psi \in \mathcal{H}$  um vetor. Então  $\psi$  pode ser escrito como combinação linear dos elementos de  $\mathcal{B}$ :  $\psi = a_1 \phi_1 + \dots + a_n \phi_n$ . Chamamos  $(a_1, \dots, a_n)$  a representação de  $\psi$  na base  $\mathcal{B}$ .

Pode-se provar que quaisquer espaços de Hilbert  $\mathcal{H}_1$  e  $\mathcal{H}_2$  de mesma dimensão são isomorfos. Assim, denotaremos um espaço de **Hilbert**  $d$ -dimensional por  $H_d$ .

Dada uma base ortonormal  $\mathcal{B}$  de um espaço de Hilbert  $\mathcal{H}$ , é fácil verificar as seguintes propriedades, para quaisquer  $\phi, \psi, \gamma \in \mathcal{H}$ :

1.  $|\phi\rangle = \sum_{\gamma \in \mathcal{B}} \langle \gamma | \phi \rangle |\gamma\rangle$
2. Se  $\langle \phi | \gamma \rangle = 0$  para todo  $\gamma \in \mathcal{B}$ , então  $\phi = 0$ .
3.  $\langle \phi | \psi \rangle = \sum_{\gamma \in \mathcal{B}} \langle \phi | \gamma \rangle \langle \gamma | \psi \rangle$
4.  $\|\psi\|^2 = \sum_{\gamma \in \mathcal{B}} |\langle \gamma | \psi \rangle|^2$  (identidade de Parseval)

Figura 104 – Propriedades numa base ortonormal de um espaço de Hilbert.

Fonte: (CARDONHA; SILVA; FERNANDES, 2004) na Definição A.10

## 7.8 Operadores lineares

Mostraremos nesta seção um tipo especial de **transformação linear** definidas sobre **espaços com produto interno**. Essas possuem propriedades que fazem com que elas sejam de muita utilidade em aplicações físicas. Na linguagem utilizada na mecânica quântica, usa-se o termo **operador** ao invés de **transformação linear**, embora representem o mesmo objeto matemático. De agora em diante, chamaremos as transformações lineares: **operadores**. A *álgebra dos operadores* aplicados à teoria

quântica é devido a **John von Neumann**.

**Definição informal** (O que é um *operador*)

Um *operador* é uma regra para transformar uma função em outra função. Tal como:  $f(x) = g(x)$ , onde  $\text{é um operador}$ .

**Exemplo** (Operador)

O operador  $\frac{d}{dx}$  transforma uma função  $f$  em sua primeira derivada  $f'$ .

### 7.8.1 Operadores e suas propriedades

A mecânica quântica tem como base à solução da **equação de Schrödinger** a qual é uma equação diferencial nas coordenadas espaciais e temporal. As grandezas físicas **observáveis** são representadas, nesta teoria, por **operadores** que é um ente matemático abstrato. Para tornar este procedimento abstrato um pouco mais concreto, é necessário aplicá-los dentro das regras da mecânica quântica, no sentido obter as grandezas físicas realmente observáveis. Este procedimento pode ser resumido pela seguinte definição:

*Definimos como **observáveis**, o conjunto  $O$  de todas aquelas grandezas reais que podem ser medidas em laboratório as quais dentro da teoria quântica são representadas por **operadores**.*

A mecânica quântica é a teoria física que obtém sucesso no estudo dos sistemas físicos cujas dimensões são próximas ou abaixo da escala atômica, tais como moléculas, átomos, elétrons, prótons e de outras partículas subatômicas. A **mecânica quântica** é formulada em termos de **operadores** sobre os espaços de **Hilbert**. E grandezas físicas observáveis são representadas, nesta nova teoria, por operadores que são entes matemáticos abstratos.

### 7.8.2 Operadores num espaço de Hilbert

**Definição** (Operador no espaço de Hilbert)

Seja  $\mathcal{H}$  um espaço de **Hilbert**. Um operador:

$$A : D(A) \subseteq \mathcal{H} \rightarrow \mathcal{H}$$

é uma aplicação que para cada elemento  $u \in D(A)$  associa um único elemento  $f \in \mathcal{H}$ , e nesse caso, indica-se  $f = Au$ . O conjunto  $D(A)$  é chamado domínio do operador  $A$ , e o conjunto:

$$R(A) = \{f \in \mathcal{H} \mid f = Au, u \in D(A)\}$$

é chamado de conjunto imagem do operador  $A$ .

**Definição** (Operador Linear)

Considere o operador  $A : D(A) \subseteq H \rightarrow H$ , onde  $D(A)$  é um subespaço vetorial de  $\mathcal{H}$ . O operador  $A$  é chamado de *operador linear* quando para quaisquer elementos  $u, v \in D(A)$  e para todo  $\alpha, \beta \in \mathbb{C}$ , tem-se:

$$A(\alpha u + \beta v) = \alpha Au + \beta Av$$

Denotaremos por  $L(H)$  o conjunto de todos os operadores lineares definidos em  $D \subseteq H \rightarrow H$ , que depende do operador  $H$ .

**Definição** (Operador Linear num espaço de **Hilbert**)

Um operador linear sobre um espaço de **Hilbert**  $\mathcal{H}$  é uma função linear tal como:

$$A : \mathcal{H} \longrightarrow \mathcal{H}.$$

A aplicação de um operador linear  $A$  em um vetor  $|\psi\rangle$  é denotada por  $A|\psi\rangle$ . Além disso,  $A$  também é um operador linear de  $\mathcal{H}^*$ , levando  $\langle\phi|$  a  $\langle\phi|A$ . Quando  $\langle\phi|A$  é aplicado a algum vetor  $\psi$ , primeiro realiza-se a aplicação de  $A$  sobre  $\psi$  para depois aplicar  $\langle\phi|$ .

Um operador linear  $A$  é chamado **positivo ou semi-definido**, denotado por  $A \geq 0$ , se, para qualquer  $|\psi\rangle \in \mathcal{H}$ , tivermos  $\langle\phi|A\psi\rangle \geq 0$ .

Fixada uma base enumerável  $\mathbf{B} = |\theta_i\rangle : i \in I$  de  $\mathcal{H}$ , qualquer operador linear  $A$  pode ser representado por uma matriz, indexada por elementos de  $I$ , tendo, como entrada  $(i, j)$ , o valor  $\langle\theta_i|A\theta_j\rangle$ . Essa matriz é identificada com o próprio operador  $A$  e denotada da mesma forma, quando não houver perigo de confusões por conta de bases diferentes.

**Definição** (Norma de um operador linear)

A norma de um operador linear  $A$  é  $\sup_{\|\phi\|=1} \|A\phi\|$ . Um operador linear  $A$  é dito limitado se  $\|A\| < \infty$ .

**Definição** (Operadores projetores)

Uma classe de operadores lineares de extrema importância são os **projetores**. Como foi visto anteriormente, se tivermos uma decomposição ortogonal de  $\mathcal{H}$  em  $W_1$  e  $W_2$ , então todo vetor de  $\psi \in \mathcal{H}$  tem uma representação única  $\psi = \psi_1 + \psi_2$ , com  $\psi_i \in W_i$ ,  $i = 1, 2$ . Os vetores  $\psi_1$  e  $\psi_2$  são as *projeções* de  $\psi$  nos subespaços  $W_1$  e  $W_2$ , respectivamente. Neste caso, o operador  $P_{W_i}$  que leva  $\psi$  a  $\psi_i$  é chamado *projetor sobre o subespaço*  $W_i$ .

Se um subespaço é gerado apenas por um vetor  $\phi$ ,  $\|\phi\| = 1$ , escrevemos  $P_\phi$ . Pode-se provar que  $P_\phi = |\phi\rangle\langle\phi|$ . Veja em ([TREFETHEN; BAU, 1997](#)).

Também não é difícil provar que todo projetor é *idempotente*, ou seja, que  $P^2 = P$ .

**Definição** (Adjunto de um operador linear)

O **adjunto**  $T^*$  de um operador linear  $T$  limitado é um operador tal que, para quaisquer  $\phi, \psi \in \mathcal{H}$ ,  $\langle \psi | T\phi \rangle = \langle T^*\psi | \phi \rangle$ . Um operador  $T$  tal que  $T^* = T$  é denominado **auto-adjunto**.

Normalmente utilizaremos a notação  $\langle \psi | T\phi \rangle$ , ao invés de  $\langle \psi T\phi \rangle$ , de modo que:

$$\langle T^*\psi | \phi \rangle = \langle \psi | T | \phi \rangle = \langle \psi | T\phi \rangle$$

Se tomarmos a matriz  $A$  correspondente ao operador linear  $T$  em relação a uma base qualquer, a matriz correspondente a  $T^*$  é simplesmente  $A^*$ , a conjugada transposta de  $A$ .

**Definição** (Matriz Adjunta). Seja  $T : U \rightarrow V$  uma transformação linear, onde  $U$  e  $V$  são espaços vetoriais com produtos internos  $\langle \cdot | \cdot \rangle_U$  e  $\langle \cdot | \cdot \rangle_V$ , respectivamente. Dizemos que uma aplicação  $T : V \rightarrow U$  é a matriz adjunta de  $T$  se esta satisfaz:

$$\langle v | T(u) \rangle_V = \langle T^*(v) | u \rangle_U, \text{ para todo } u \in U, v \in V.$$

**Proposição** (Unicidade da  $T^*$  Adjunta). Seja  $T : U \rightarrow V$  uma transformação linear, onde  $U$  e  $V$  são espaços vetoriais com produtos internos  $\langle \cdot | \cdot \rangle_U$  e  $\langle \cdot | \cdot \rangle_V$ , respectivamente. Caso exista  $T^*$ , esta é única.

**Proposição** ( $T^*$  é linear). Seja  $T : U \rightarrow V$  uma transformação linear, onde  $U$  e  $V$  são espaços vetoriais com produtos internos  $\langle \cdot | \cdot \rangle_U$  e  $\langle \cdot | \cdot \rangle_V$ , respectivamente. Caso exista  $T^*$ , esta é *linear*.

As demonstrações destas proposições estão em (CARDONHA; SILVA; FERNANDES, 2004).

## 7.9 Bibliografia e Fonte de Consulta

Teoria dos Corpos - <[https://pt.wikipedia.org/wiki/Teoria\\_dos\\_corpos](https://pt.wikipedia.org/wiki/Teoria_dos_corpos)>.

Corpo algébrico - <[https://pt.wikipedia.org/wiki/Corpo\\_matematico](https://pt.wikipedia.org/wiki/Corpo_matematico)>.

Callioli, Carlos A.; Hygino H. Domingues; Roberto C. F. Costa. Álgebra Linear e Aplicações. 6 ed. São Paulo: Atual, 1990. ISBN 9788570562975.

Noble, Ben; James W. Daniel. Álgebra Linear Aplicada. Rio de Janeiro: Prentice-Hall do Brasil, 1986. ISBN 9788570540225.

Norma matemática - <[https://pt.wikipedia.org/wiki/Norma\\_matematica](https://pt.wikipedia.org/wiki/Norma_matematica)>

Cálculo das Variacões - <[https://pt.wikipedia.org/wiki/Calculo\\_de\\_variacoes](https://pt.wikipedia.org/wiki/Calculo_de_variacoes)>

Espaço Métrico - <[https://pt.wikipedia.org/wiki/Espaco\\_metrico](https://pt.wikipedia.org/wiki/Espaco_metrico)>

Espaço de Manhattan (Taxicab Geometry) - <[https://en.wikipedia.org/wiki/Taxicab\\_](https://en.wikipedia.org/wiki/Taxicab_)

[geometry](#)>

Espaço Topológico - <[https://pt.wikipedia.org/wiki/Espaco\\_Topologico](https://pt.wikipedia.org/wiki/Espaco_Topologico)>

## 7.10 Referências e Leitura Recomendada

Espaços de Hilbert - Gislan Silveira Santos, Vitória da Conquista, BA, Julho de 2008  
<<http://www.ebah.com.br/content/ABAAAAXhcAJ/espacos-hilbert?part=3>>





# Espaços de Hilbert e a Teoria Quântica

**J**ohn von Neumann, nome original **János Neumann**, nascido em 28 de dezembro de 1903, Budapeste, Hungria, morreu em 8 de fevereiro de 1957, Washington, D.C., USA. Quando adulto, ele anexou *von* ao seu sobrenome: o título hereditário fora concedido a seu pai em 1913. **Von Neumann** cresceu de criança prodígio para um dos matemáticos mais proeminentes do mundo aos seus vinte e cinco anos. Um trabalho importante na teoria dos conjuntos de **Georg Cantor**, inaugurou uma carreira que tocou quase em todos os principais ramos da matemática. O dom de **John von Neumann** para a matemática aplicada levou seu trabalho a direções que influenciaram a **teoria quântica**.

**Carreira Europeia, 1921-1930** - **Von Neumann** iniciou sua carreira intelectual numa época em que a influência de **David Hilbert** e seu programa de estabelecimento de fundamentos axiomáticos para a matemática estava no auge. Um artigo de **von Neumann**, escrito enquanto ainda estava no Lutheran Gymnasium ("Introduction of Transfinite Ordinals", publicado em 1923), forneceu a definição agora convencional de um número ordinal como o conjunto de todos os números ordinais menores. Isso evita algumas das complicações levantadas pelos números transfinitos de **Georg Cantor**. "Axiomatization of Set Theory" de **Von Neumann** (1925) despertou a atenção do próprio **Hilbert**. De 1926 a 1927, **von Neumann** fez um trabalho de pós-doutorado sob a orientação de **Hilbert** na Universidade de Göttingen. O objetivo de axiomatizar a matemática foi derrotado pelos teoremas de incompletude de **Kurt Gödel**, uma barreira que foi entendida imediatamente por **Hilbert** e **von Neumann**. Em meados dos anos 20, **von Neumann** se viu apontado como um prodígio em conferências. (Ele alegou que os poderes matemáticos começam a declinar aos 26 anos, após os quais a experiência pode ocultar a deterioração por um tempo.) Von Neumann produziu uma sucessão impressionante de artigos fundamentais em *lógica*, *teoria dos conjuntos*, *teoria dos grupos*, *teoria ergódica* e *teoria dos operadores*. **Herman Goldstine** e **Eugene Wigner** notaram que, de todos os principais ramos da matemática, foi apenas na topologia e na teoria dos números que **von Neumann** não conseguiu dar uma contribuição importante. Em 1929, **von Neumann** foi convidado a dar uma palestra sobre **teoria quântica** na Universidade de Princeton. Isso o levou a uma nomeação como professor visitante (1930-1933).

**Princeton, 1930-1942** - Em 1933, Adolf Hitler chegou ao poder na Alemanha, e **John von Neumann** renunciou a seus cargos acadêmicos alemães. No mesmo ano, **John von Neumann** tornou-se um dos primeiros professores do *Institute for Advanced Study* (IAS - <<https://www.ias.edu>>), em Princeton, New Jersey, USA. Motivado por um desejo contínuo de desenvolver técnicas matemáticas adequadas aos **fenômenos quânticos**, **John von Neumann**, de 1929 até a década de 1940, introduziu a *teoria de álgebra de operadores*, agora conhecida como *álgebras de von Neumann*.

## 8.1 Espaços Vetorial nos Números Complexos

O conjunto das n-uplas  $(z_0, \dots, z_{n-1})$  de números complexos com a **soma** e o **produto por escalar** definidos é um Espaço Vetorial Complexo e é denotado por  $\mathbb{C}^n$ . É conveniente representar esses elementos por vetores coluna. Tem-se então:

$$\begin{bmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{bmatrix} + \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{n-1} \end{bmatrix} = \begin{bmatrix} z_0 + w_0 \\ z_1 + w_1 \\ \vdots \\ z_{n-1} + w_{n-1} \end{bmatrix} \quad \text{e} \quad z \cdot \begin{bmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{bmatrix} = \begin{bmatrix} z \cdot z_0 \\ z \cdot z_1 \\ \vdots \\ z \cdot z_{n-1} \end{bmatrix}$$

Na teoria quântica, os vetores de  $\mathbb{C}^n$  costumam ser usados na notação de **Dirac** (**DIRAC, 1939**):

$$|\psi_i\rangle = (z_0, z_1, \dots, z_{n-1}) = \begin{bmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{bmatrix}$$

Os vetores se comportam de maneira semelhante aos números no que diz respeito à soma e subtração. Em particular, a soma é comutativa:  $|\phi\rangle + |\psi\rangle = |\psi\rangle + |\phi\rangle$ , há um vetor nulo denotado por  $0$  ou  $|\phi\rangle = (0, 0, \dots, 0, 0)$  de tal forma que  $|\psi\rangle + 0 = |\psi\rangle$  e ainda vale  $-|\psi\rangle = (-z_0, \dots, -z_{n-1}) = -1 \cdot |\psi\rangle$ .

O **produto por escalar** também se comporta de maneira semelhante ao produto numérico, e valem as propriedades distributivas:

$$z \cdot (|\phi\rangle + |\psi\rangle) = (z \cdot |\phi\rangle + z \cdot |\psi\rangle) \quad \text{e} \quad (z + w) \cdot |\psi\rangle = z \cdot |\psi\rangle + w \cdot |\psi\rangle.$$

**Exemplo 8.1 (Espaço de estados de 1 qubit):** O espaço  $\mathbb{C}^2$  O conjunto

$$\mathbb{C}^2 = \left\{ |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \right\}, \quad \text{onde } \alpha, \beta \in \mathbb{C}.$$

é um espaço vetorial com soma e produto por escalar dados por:

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = [ a_1 + b_1, a_2 + b_2 ]$$

e

$$z \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} z \cdot a \\ z \cdot b \end{bmatrix}$$

Esse espaço vetorial  $\mathbb{C}^2$  descreve o espaço de estados de 1 *qubit* para a computação quântica, e será largamente utilizado nas seções seguintes.

## 8.2 Bases e Dimensão

Uma *base* para o espaço vetorial  $\mathbb{C}^n$  é um conjunto de vetores *linearmente independentes* e que geram o espaço. Demonstra-se que todas as bases de um espaço vetorial têm o mesmo número de elementos, e define-se a dimensão do espaço vetorial pelo número de elementos de uma base.

O espaço vetorial  $\mathbb{C}^n$  tem dimensão  $n$ , isto é, todas as suas bases têm  $n$  vetores. Uma *base* muito útil é a chamada *base computacional*, ou **base canônica**<sup>1</sup>

Em computação quântica, utilizam-se **estados quânticos** em vez de **estados clássicos**. O bit é, então, substituído pelo bit quântico, um qubit, e os valores 0 e 1 de um bit clássico são substituídos pelos vetores quânticos de estados  $|0\rangle$  e  $|1\rangle$ , representados por:

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

Essa notação, utilizada em mecânica quântica, é conhecida por notação de **Dirac**. A diferença entre um *bit* e um *qubit* é que um *qubit* genérico  $|\psi\rangle$  pode também ser uma combinação linear dos vetores  $|0\rangle$  e  $|1\rangle$ , ou seja:

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

onde  $\alpha$  e  $\beta$  são números complexos. Note que os vetores  $|0\rangle$  e  $|1\rangle$  formam uma base ortonormal do espaço vetorial  $\mathbb{C}^2$ . Essa base é chamada de *base computacional* e o vetor  $|\psi\rangle$  é chamado de superposição/sobreposição dos vetores de estados  $|0\rangle$  e  $|1\rangle$ , com amplitudes probabilísticas  $\alpha$  e  $\beta$ . Em mecânica quântica, esse vetor é também chamado de *estado quântico* genérico. Usaremos os dois termos (sobreposição/superposição ou estado quântico genérico) com o mesmo significado.

As amplitudes aqui, dizem respeito a *amplitude de uma onda* que é a medida da magnitude de um distúrbio em um meio, durante um ciclo de onda, que equivalem neste modelo, aos números complexos  $\alpha$  e  $\beta$ .

A interpretação física do *qubit*  $|\psi\rangle$  é que ele está simultaneamente nos estados  $|0\rangle$  e  $|1\rangle$ . Isso faz com que a quantidade de informação que pode ser armazenada no estado  $|\psi\rangle$  seja infinita. Entretanto, essa informação está no nível quântico, sem ser

<sup>1</sup> O adjetivo "canônico", na Matemática, tem um sentido de "padrão", como na expressão "configuração padrão".

acessível. Para torná-la acessível, no nível clássico, precisamos fazer uma medida. Mas, a mecânica quântica diz que o processo de medida altera o estado de um qubit, fazendo-o assumir o estado  $|0\rangle$ , com probabilidade  $|\alpha|^2$ , ou o estado  $|1\rangle$ , com probabilidade  $|\beta|^2$  (isso significa que os valores  $\alpha$  e  $\beta$  não podem ser conhecidos através de uma medida). Então, com apenas duas possibilidades,  $|0\rangle$  ou  $|1\rangle$ , temos, então:

$$|\alpha|^2 + |\beta|^2 = 1$$

Isso significa que a norma do vetor  $|\psi\rangle$  vale 1 (vetor unitário). Resumindo: matematicamente, um *qubit* é um vetor de norma 1 de  $\mathbb{C}^2$ .

Na verdade, a *definição da base computacional* deveria ser:

$$|0\rangle = \begin{pmatrix} (1, 0) \\ (0, 0) \end{pmatrix} \text{ e } |1\rangle = \begin{pmatrix} (0, 0) \\ (1, 0) \end{pmatrix}$$

pois todas as coordenadas de  $|0\rangle$  e  $|1\rangle$  são os números complexos  $1 + 0i$  e  $0 + 0i$  para  $|0\rangle$ , com  $0 + 0i$  e  $1 + 0i$  para  $|1\rangle$ . Para simplificar a notação, usou-se 1 para representar  $(1, 0)$  e 0 para representar  $(0, 0)$ .

Na equação  $|\alpha|^2 + |\beta|^2 = 1$ , considere  $\alpha = a + i.b$  ( $a, b \in \mathbb{R}$ ) e  $\beta = c + i.d$  ( $c, d \in \mathbb{R}$ ). Como  $|\alpha|^2 + |\beta|^2 = 1$ , podemos escrever que  $a^2 + b^2 + c^2 + d^2 = 1$ . Nesse caso, podemos interpretar um *qubit* como sendo um vetor unitário de  $\mathbb{R}^4$ .

Entretanto, existe uma representação geométrica de um *qubit* em  $\mathbb{R}^3$ : a esfera de **Bloch**. Note que  $\mathbb{C}$  é equivalente ao espaço de coordenadas  $\mathbb{R}^2$ , e então  $\mathbb{C}^2$  equivale ao  $\mathbb{R}^3$ , como se fossem dois planos ortogonais  $\mathbb{C}$ .

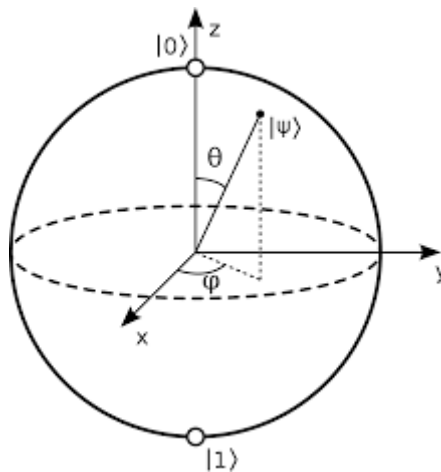


Figura 105 – A esfera de Bloch mostra uma representação de um *qubit*, o bloco de construção fundamental de computadores quânticos, representado na superfície de uma esfera de raio 1.

Fonte: Wikipedia

**Espaços de Hilbert** desempenham um papel fundamental em toda a Teoria Quântica e em várias áreas da Matemática. Na Teoria Quântica, por exemplo, um sistema físico é descrito por um **Espaço de Hilbert** sobre o **corpo** dos números complexos, que contém os *vetores de estados quânticos*, e todas as informações do sistema e suas complexidades. Por isto, forma a base matemática de qualquer pesquisa em direção ao estudo da **criptografia quântica**, a área da computação quântica mais pesquisada e desenvolvida. Para os pretendentes em *criptografia quântica*, deve-se começar com a definição de um **Espaço de Hilbert**.

Um espaço de **Hilbert** é uma generalização de um espaço euclidiano que não precisa estar restrito a um número finito de dimensões. É um espaço dotado de um produto interno, apresentado as noções de distância e ângulos. Os elementos são chamados de vetores, os quais na teoria quântica representam informações completas sobre um estado físico, apresentados sob a notação de **Dirac** (NIELSEN; CHUANG, 2000).

Um **sistema quântico** é representado por um espaço de **Hilbert**  $\mathcal{H}$  com a dimensão escolhida, apropriadamente. Para sua aplicação à computação quântica, esta dimensão sempre será finita de tamanho  $n$ . Se tivermos dois sistemas quânticos com seus correspondentes espaços de **Hilbert**  $\mathcal{H}_1$  e  $\mathcal{H}_2$ , então o espaço de **Hilbert** correspondente à composição destes sistemas será  $\mathcal{H} := \mathcal{H}_1 \otimes \mathcal{H}_2$ , que correspondente ao *produto tensorial* entre os vetores de  $\mathcal{H}_1$  e  $\mathcal{H}_2$ .

Um computador quântico é sistema quântico, um dispositivo que executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como *sobreposição* e *interferência*. Em computação quântica, utilizam-se **estados quânticos** em vez de **estados clássicos**. O bit é, então, substituído pelo bit quântico, um *qubit*, e os valores 0 e 1 de um bit clássico são substituídos pelos vetores quânticos de estados  $|0\rangle$  e  $|1\rangle$ .

Dois das noções mais importantes nas teorias físicas são as de **estado** e a de **grandeza física**, quantidade ou magnitude física. De um modo geral, estados são caracterizações básicas dos objetos físicos tratados pela teoria. As grandezas físicas são as *propriedades mensuráveis* desses objetos, são representadas por *funções*. Exemplos simples seriam a posição,  $r$ , o momentum  $p$  (que são as grandezas que entram na composição do estado) de um objeto, a energia cinética e a energia potencial armazenada numa mola, por exemplo.

**Estados** em geral evoluem com o tempo, em virtude de ações exercidas sobre o corpo. Na mecânica clássica, a equação fundamental que rege essa evolução é, como se sabe, a segunda lei de Newton,  $F = m.a$ . Essa evolução temporal é completamente determinística, ou seja, dado um estado inicial,  $(r_0, p_0)$ , e as forças que agem sobre o objeto, a equação permite, em princípio, o cálculo do estado num outro instante  $t$  qualquer,  $(r_t, p_t)$ . Passemos agora à situação na mecânica quântica. Um **estado quântico** é qualquer estado possível em que um sistema mecânico quântico possa se encontrar. Um *estado quântico* plenamente especificado pode ser descrito por um *vetor de estado*, por uma *função de onda* ou por um *conjunto completo de números quânticos* para um dado sistema. Ao estado quântico de menor energia possível dá-se o nome de *estado quântico fundamental*.

## 8.3 Postulados da mecânica quântica

Nesta seção, o leitor poderá ver com todos os detalhes em (COURTEILLE, 2017). Cinco postulados estão explicados nesta referência, nas páginas 9-13.

### Princípio de superposição (Postulado 1)

Um sistema físico pode se encontrar em vários estados, simultaneamente. Na mecânica quântica, cada estado possível é descrito por uma função de onda  $\psi$ . As funções de ondas podem ser funções de vários tipos de coordenadas, por exemplo da posição  $\psi = \psi(r)$ , do momento  $\psi = \psi(p)$  ou da energia  $\psi = \psi(E)$ . A escolha das coordenadas se chama *representação*.

Existem sistemas que só podem existir num número restrito de estados, como o átomo de dois níveis. Outros podem existir num número infinito de estados ou mesmo numa distribuição contínua de estados.

**Schrödinger** inventou a *mecânica das ondas* quando derivou a sua equação de ondas à partir da relação de dispersão para partículas massivas. **Heisenberg** inventou a mecânica (detalhada nas últimas seções) que ele chamou de *mecânica das matrizes*. Mais tarde ele mostrou a equivalência formal das duas teorias.

### Interpretação da função de onda (Postulado 2)

A função de estado (ou função de onda) caracteriza um sistema do qual podemos calcular várias propriedades. A função pode adotar valores complexos destituídos de interpretação física imediata. De fato, a função de onda é sobretudo um construto matemático.

**Uma função de onda não é uma onda real associada a uma partícula. Ela não tem qualquer sentido físico direto. Trata-se apenas de uma abstração (representação) matemática.**

A *onda* da **função de onda**, no entanto, não é uma onda no espaço físico; é uma *onda* em um "*espaço matemático abstrato*".

Por outro lado, a norma  $\|\psi\|^2$  tem o significado de uma probabilidade do sistema de estar no estado  $\psi$ . Isso é a famosa interpretação de **Max Born** da função de onda.

Se  $\psi_k$ , com  $k = 1, 2, \dots$  são todos os estados possíveis de um sistema, a interpretação como probabilidade requer  $\sum_k |\psi_k|^2 = 1$ .

Isto é, a *probabilidade* precisa de **normalização**.

### Observáveis (Postulado 3)

O único jeito de achar informações sobre um sistema consiste em medir os valores de grandezas características do sistema. Na mecânica quântica descrevemos grandezas físicas observáveis por operadores agindo sobre o espaço de Hilbert das funções de onda, e cada sistema quântico é completamente descrito por um conjunto completo de observáveis. Para distinguir melhor os *observáveis*, colocamos um "acento

circunflexo" no símbolo representando o *observável*.

Postulamos a substituição das variáveis dinâmicas caracterizando um sistema clássico por objetos abstratos chamado **operadores**.

### Princípio de correspondência (Postulado 4)

*Operadores* não necessariamente comutam.

### Equação de Schrödinger e medidas quânticas (Postulado 5)

Na mecânica quântica, a **equação de Schrödinger** é uma equação diferencial parcial que descreve **como o estado quântico de um sistema físico muda com o tempo**. Foi formulada no final de 1925, e publicada em 1926, pelo físico austríaco **Erwin Schrödinger**.

Na mecânica clássica, a equação de movimento é a segunda lei de Newton, ( $F = m \cdot a$ ) utilizada para prever matematicamente o que o sistema fará a qualquer momento após as condições iniciais do sistema. Na mecânica quântica, o análogo da lei de **Newton** é a **equação de Schrödinger** para o sistema quântico (geralmente átomos, moléculas e partículas subatômicas sejam elas livres, ligadas ou localizadas).

Não é uma equação algébrica simples, mas, em geral, uma **equação diferencial parcial linear**, que descreve o tempo de evolução da **função de onda** do sistema (também chamada de "função de estado").

A *onda* da **função de onda**, no entanto, não é uma onda no espaço físico; é uma *onda* em um "*espaço matemático abstrato*".

Há *uma função de onda* para todo o sistema, e não uma função de onda para cada partícula individual em certo sistema. Partículas elementares, como os elétrons, têm *spin*, e a função de onda deve incluir essa propriedade fundamental como um grau de liberdade intrínseca.

A mecânica clássica apenas assume o aspecto corpuscular (em forma de partícula), donde é compreensível que não possa descrever a dinâmica das partículas materiais nos casos em que os aspectos ondulatórios sejam importantes. Assim, em tais situações, as equações clássicas de **Newton**, ou de **Hamilton**, terão de ser substituídas por equações mais gerais que englobem a natureza dual da matéria ([FERNANDES, 2010](#)).

Uma delas é a equação de **Schrödinger** dependente do tempo  $t$ . Usando a notação de Dirac ([DIRAC, 1939](#)), o vetor de estados em um instante  $t$ , dado por  $|\psi(\vec{x}, t)\rangle$  é qualquer estado quântico em que o sistema possa se encontrar. A equação de **Schrödinger** dependente do tempo, então, escreve-se:

$$\hat{H} |\psi(\vec{x}, t)\rangle = i\hbar \frac{\partial}{\partial t} |\psi(\vec{x}, t)\rangle$$

onde  $\hat{H}$  é o operador **Hamiltoniano auto-adjunto** atuando no vetor de estados  $|\psi(\vec{x}, t)\rangle$  (**função de onda**),  $i = \sqrt{-1}$  e  $\hbar = h/2\pi$  é a **constante de Planck**  $h$ , **reduzida**. A **função de onda** define, neste contexto, o **estado do sistema**



**quântico**, e dela se pode obter toda a informação que é possível conhecer sobre o sistema. A existência do número imaginário  $i$  na equação, antecipa que a **função de onda** (soluções da equação) podem ser complexas. Como tal é importante uma revisão de alguns aspectos da análise complexa (ver o texto T5 em (FERNANDES, 2010)). Um operador representa uma ação sobre uma dada função produzindo uma nova função. Em mecânica quântica, as propriedades físicas observáveis são sempre representadas por operadores. O **Hamiltoniano**  $\hat{H}$  é o operador que representa a energia total do sistema (energia cinética + energia potencial). Assim como a força na segunda Lei de Newton, ele não é definido pela equação e deve ser determinado pelas propriedades físicas do sistema.

**Schrödinger** estabeleceu a sua equação a partir do caso, muito particular, de uma partícula livre (isto é, não sujeita a um potencial), e assumiu que a equação é válida em todas as situações. Portanto, tal como a equação de Newton,  $F = m.a$ , não existe uma demonstração cabal para essa equação. A sua justificativa reside apenas no acordo entre as previsões que dela se deduzem e os resultados experimentais. Assim, deve ser considerada como um postulado da teoria quântica (FERNANDES, 2010).

Desta forma, podemos dizer que: resolver a equação de **Schrödinger** é encontrar os *autovalores* e **autofunções** do operador **Hamiltoniano** do sistema. Os *autovalores* de um dado operador **Hamiltoniano** representam as grandezas físicas *observáveis* permitidas.

## 8.4 Operadores na mecânica quântica

Os operadores que correspondem a grandezas físicas em mecânica quântica são lineares.

Na formulação da **mecânica quântica** se destacam **duas classes de operadores lineares**:

- operadores hermitianos.
- operadores unitários.

**Definição** (Operador Hermitiano)

Seja um espaço de **Hilbert**  $\mathcal{H}$ , e  $\hat{H}$  é um operador. Esse operador  $\hat{H}$  é chamado de **hermitiano** (no caso em que o corpo do espaço vetorial  $K = \mathbb{C}$ ), desde que para todo  $\psi$  e  $\phi$  se satisfaça que:

$$\langle \psi | \hat{H} \phi \rangle = \langle \hat{H} \psi | \phi \rangle$$

Vale lembrar que o produto interno  $\langle \psi | \hat{H} \phi \rangle = \langle \hat{H} \psi | \phi \rangle \in \mathbb{C}$ .

Uma matriz  $A$  é **hermitiana** se  $A = A^*$ . A cada operador auto-adjunto  $T$  corresponde uma matriz hermitiana  $A$ .

**Definição** (O que é um Autovalor)

Um **autovalor** é o valor que se obtém ao se aplicar algum operador a um estado de modo que o resultado da operação seja o próprio estado multiplicado pelo autovalor.

**Definição** (O que é um Observável)

Em mecânica quântica, um **observável** é um **operador** que, aplicado ao estado de um sistema, produz como **autovalores** os possíveis valores de alguma grandeza passível de mensuração. Todos os **observáveis** são representados por **operadores hermitianos**.

**Definição** (Operadores ortogonais e unitários)

Seja um **espaço de Hilbert**  $\mathcal{H}$  e um operador  $\hat{U} : \mathcal{H} \rightarrow \mathcal{H}$ . Esse operador é chamado de **ortogonal**, no caso em que  $\mathcal{K} = \mathbb{R}$ , ou **unitário**, no caso em que  $\mathcal{K} = \mathbb{C}$ , desde que preserve o **produto interno**. Isso quer dizer que vale:

$$\langle \hat{U}\psi | \hat{U}\phi \rangle$$

**Definição** (Matriz Ortogonal e Matriz Unitária)

Uma **matriz quadrada real** é chamada de **ortogonal** desde que a sua **inversa** seja a sua **transposta**, e uma **matriz quadrada complexa** é chamada de **unitária** desde que a sua **inversa** seja a sua **transposta conjugada**.

É interessante estudar o que acontece com as matrizes associadas a **operadores unitários** em **bases ortonormais**. Para isso vamos enunciar a seguinte propriedade:

Seja um espaço de **Hilbert**  $\mathcal{H}$  e um **operador unitário** (ou **ortogonal**). Seja  $B = \{\xi_1, \xi_2, \dots, \xi_n\}$ . Então, uma base ortonormal de  $\mathcal{H}$  é  $U_{BB}$  que define uma matriz unitária (ou ortogonal).

Podemos verificar que se  $\hat{U}$  é um **operador unitário**, ele tem como consequência a preservação do produto interno dos operadores unitários, preservam a norma de um vetor, a distância entre vetores e o ângulo entre vetores.

**Definição** (Operadores simétricos e hermitianos)

Seja um **espaço de Hilbert**  $\mathcal{H}$  e um operador  $\hat{H} : \mathcal{H} \rightarrow \mathcal{H}$ . Esse operador é chamado de **simétrico** (no caso  $\mathcal{K} = \mathbb{R}$ ), ou **hermitiano** (no caso  $\mathcal{K} = \mathbb{C}$ ), desde que para todo  $\psi$  e  $\phi$ , se satisfaça que  $\langle \psi | \hat{H}\phi \rangle = \langle \hat{H}\psi | \phi \rangle$ . Vale a pena lembrar que o produto interno  $\langle \psi | \hat{H}\phi \rangle = \langle \hat{H}\psi | \phi \rangle \in \mathcal{K}$ .

**Definição** (Matriz Simétrica) (SANTOS, 2016)

Chamamos de matriz simétrica à matriz  $A(m \times m)$ , tal que  $A(m \times m) = A^T(m \times m)$ .

Isso implica em:

a)  $a_{ij} = a_{ji}$ , ou seja, seus elementos são simetricamente organizados em relação à diagonal principal.

b) O produto  $A.A^T$  produz uma matriz simétrica.

Se a matriz simétrica possuir apenas elementos formados por números reais (chamada de matriz simétrica real) são válidas as seguintes propriedades:

**Propriedade 1)** Todos os autovalores de uma matriz simétrica real são reais

**Propriedade 2)** Autovetores associados a autovalores distintos são ortogonais.

**Definição** (Matriz Hermitiana)

**Matrizes Hermitianas** (SANTOS, 2016)- As **matrizes hermitianas** são uma extensão das matrizes reais simétricas. No sistema complexo dizemos que uma **matriz quadrada é hermitiana** quando é igual a sua **conjugada transposta**, ou seja,  $A = A^*$ .

Tomemos, por exemplo, a matriz quadrada  $A$ , de ordem 2.

$$A = \begin{bmatrix} a_1 + i.a_2 & b_1 + i.b_2 \\ c_1 + i.c_2 & d_1 + i.d_2 \end{bmatrix}$$

A **conjugada transposta** é dada por:

$$A^* = \begin{bmatrix} \overline{a_1 + i.a_2} & \overline{b_1 + i.b_2} \\ \overline{c_1 + i.c_2} & \overline{d_1 + i.d_2} \end{bmatrix}$$

$$A = \begin{bmatrix} a_1 - i.a_2 & c_1 + i.c_2 \\ b_1 + i.b_2 & d_1 - i.d_2 \end{bmatrix}$$

Se  $A$  é **Hermitiana**, então  $A = A^*$ . Logo, concluímos que:

$$A = \begin{bmatrix} a_1 & b_1 + i.b_2 \\ b_1 - i.b_2 & d_1 \end{bmatrix}$$

Podemos expandir esse resultado para matrizes de ordem  $n$ . Dessa maneira, se uma matriz  $A$  é **hermitiana**, então são válidas as seguintes afirmações:

a) Os elementos da diagonal principal de  $A$  são números reais.

b) O elemento  $a_{ij}$  na  $i$ -ésima linha e na  $j$ -ésima coluna é o **conjugado complexo** do elemento que está na  $j$ -ésima linha e na  $i$ -ésima coluna.

Em homenagem a **Charles Hermite** (1822-1901), matemático francês, quem foi

o primeiro a utilizar a terminologia "Matrizes Ortogonais" e a mostrar que se uma matriz é igual a sua própria **conjugada transposta**, então seus autovalores serão reais.



Figura 106 – Charles Hermite - Foi o primeiro a utilizar a terminologia "Matrizes Ortogonais" e criador das matrizes hermitianas.

Fonte: Wikipédia, a enciclopédia livre. Disponível em:  
<[https://pt.wikipedia.org/wiki/Charles\\_Hermite](https://pt.wikipedia.org/wiki/Charles_Hermite)>. Acesso em: 03 Abr. 2019.

É interessante estudar o que acontece com as matrizes associadas a **operadores simétricos** (no caso  $\mathcal{K} = \mathbb{R}$ ) ou **hermitianos** (no caso  $\mathcal{K} = \mathbb{C}$ ) em **bases ortonormais**. Para isso, vamos enunciar a seguinte propriedade:

Seja um **espaço de Hilbert**  $\mathcal{H}$  e um **operador simétrico** (ou **hermitiano**)  $\hat{H}$ , seja  $B = \{\xi_1, \xi_2, \dots, \xi_n\}$  uma base ortonormal de  $\mathcal{H}$ , então  $H_{BB}$  é uma matriz **hermitiana** (ou **simétrica**).

**Exemplos:**

$$A = \begin{bmatrix} 1 & 5 - 2i \\ 5 + 2i & 5 \end{bmatrix}$$

**Esta matriz não é hermitiana** pois apresenta elementos com a unidade imaginária na diagonal principal.

$$A = \begin{bmatrix} 0 & 5 - 2i \\ 5 - 2i & 5 \end{bmatrix}$$

É uma **matriz simétrica**, mas **não é hermitiana** pois o elemento da primeira linha e segunda coluna não é o conjugado do elemento da segunda linha e primeira coluna.

$$A = \begin{pmatrix} 7 & 3 - i & -5i \\ 3 + i & 0 & 1 - 3i \\ 5i & 1 + 3i & 0 \end{pmatrix}$$

é uma **matriz hermitiana**.

Toda **matriz real simétrica** é também uma **matriz hermitiana**, pois satisfaz as propriedades enunciadas.

## 8.5 Problema de autovalores e autovetores

O problema de **autovalores e autovetores de um operador** é muito importante em diversas áreas da Física. Trata-se de encontrar vetores não nulos de um espaço vetorial e escalares tal que, se satisfaça a seguinte relação :

$$\psi = \lambda \psi, \text{ com } \psi \in \mathcal{H}.$$

A equação acima é conhecida pelo nome de **equação de autovalores e autovetores** do operador . Embora não seja necessário, suporemos que o nosso espaço vetorial possui produto interno, já que é esse o caso de maior interesse na Física (BUTKOV, 1968) (BOLDRINI et al., 1980).

### Autovalores e Autovetores de uma Matriz

Um operador admite uma representação matricial. Por conta disso, vamos introduzir o problema em termos de matrizes.

**Definição** (Autovetor de uma matriz)

Dada uma matriz  $A \in \mathcal{K}^{n \times n}$ , dizemos que a matriz coluna não nula  $x \in \mathcal{K}^{n \times 1}$  é **autovetor da matriz**  $A$ , desde que se satisfaça a relação

$$Ax = \lambda x, \text{ com } \lambda \in \mathcal{K}$$

onde  $\lambda$  é conhecido pelo nome de **autovalor** correspondente (ou associado) ao **autovetor**  $x$ . A equação acima pode ser escrita também, da forma

$$Ax - \lambda x = 0$$

onde  $0$  é a matriz coluna nula de  $\mathcal{K}^{n \times 1}$ , ou ainda

$$Ax - \lambda \mathbb{I}x = 0 \text{ ou } (A - \lambda \mathbb{I})x = 0$$

sendo que  $\mathbb{I}$  é a matriz identidade de  $\mathcal{K}^{n \times n}$  (BUTKOV, 1968) (BOLDRINI et al., 1980).

## 8.6 Operador Hamiltoniano

**William Rowan Hamilton** (1805-1865) foi um matemático, físico e astrônomo irlandês. Contribuiu com trabalhos fundamentais ao desenvolvimento da álgebra, da Física, e é muito conhecido pelo seu trabalho que veio a ser influente nas áreas da mecânica quântica e da teoria quântica de campos. Em sua homenagem são designados os **operadores hamiltonianos**, por ele inventados.



Figura 107 – W. R. Hamilton - Operador Hamiltoniano, Autofunções e Autovalores.

Fonte: [https://pt.wikipedia.org/wiki/William\\_Rowan\\_Hamilton](https://pt.wikipedia.org/wiki/William_Rowan_Hamilton)

Um **Hamiltoniano**  $\hat{H}$  é um *operador observável* cujos *autovalores* são as possíveis energias do sistema. O **Hamiltoniano**  $\hat{H}$  é um operador cujo observável correspondente à energia total do sistema. Como todos os observáveis, o **espectro do Hamiltoniano** é o conjunto de possíveis resultados quando mede-se a energia total de um sistema.

Os estados quânticos que permitem que isso ocorra são os *auto-estados* daquele operador. Quando acontece de diferentes estados quânticos possuírem o mesmo autovalor para um dado operador, tal autovalor é dito "degenerado". Então aquele operador não permite identificar o estado em que o sistema se encontra. Para conseguir isso é preciso aplicar outro operador que tenha os mesmos auto-estados mas para o qual os auto-estados exibam autovalores distintos. Operadores que tenham os mesmos auto-estados são os que comutam entre si, ou seja, que o resultado da ação conjunta deles seja independente da ordem em que sejam aplicados.

Fisicamente, aplicar um *operador* a um *estado quântico* significa preparar um sistema e aplicar uma ação que provoque alguma alteração. Os **auto-estados do Hamiltoniano** podem ser percebidos se medirmos a energia do sistema quântico pela aplicação. Por exemplo, de um campo elétrico. Já o *momento angular* pode ser observado pela aplicação de um campo magnético, que divide os **estados degenerados do Hamiltoniano** nos subestados do *momento angular*, o que é chamado de "estrutura fina" das raíes espectrais reveladoras das energias dos estados do sistema quântico. Ver em: **Ernesto von Rückert** em <<https://ask.fm/wolfedler/answers/127199746077>>.

Em mecânica quântica, o **Hamiltoniano**  $\hat{H}$  é um operador cujo observável correspondente à energia total do sistema. Como todos os observáveis, o **espectro do Hamiltoniano** é o conjunto de possíveis resultados, quando mede-se a **energia total** de um sistema.

O que é momento linear? Trata-se de uma grandeza que mede a quantidade de movimento presente em um corpo.

O **operador momento linear** segundo o eixo dos x:  $\hat{p}_x = -i\hbar \frac{\partial}{\partial x}$ , (expressões análogas para as componentes y e z), onde  $i = \sqrt{-1}$  e  $i^2 = -1$ .

O **operador posição** segundo o eixo dos x:  $\hat{x} = x$  (expressões análogas para as componentes y e z).

O **Hamiltoniano** clássico, para o caso particular de uma única partícula material a mover-se segundo o eixo dos x (uma generalização pode ser feita para o espaço tridimensional e para um sistema de partículas)

$$H(p_x, x) = \frac{p_x^2}{2m} + U(x)$$

ou seja, a energia total da partícula, E (soma das energias cinética e potencial).

De acordo com as regras anteriores, o respectivo operador **Hamiltoniano** é:

$$\hat{H}(\hat{p}_x, \hat{x}) = \frac{\hat{p}_x^2}{2m} + U(\hat{x}) = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2}$$

Assim, a **equação de Schrödinger** para este caso particular é:

$$-\frac{\hbar^2}{2m} \frac{\partial^2 \Psi(x,t)}{\partial x^2} + U(x)\Psi(x,t) = i\hbar \frac{\partial \Psi(x,t)}{\partial t}$$

Conhecida a energia potencial  $U(x)$  tudo o que há a fazer é resolver esta equação diferencial de modo a encontrar as suas soluções: as funções de onda  $\Psi(x, t)$  que definem os estados quânticos da partícula, os quais contêm toda a informação física que é possível obter.

Note-se que se energia potencial for independente do tempo, um dos termos da equação está apenas relacionado com a parte espacial (depende de  $x$ ), e o outro com o aspecto temporal (depende de  $t$ ).

$$\begin{aligned} -\frac{\hbar^2}{2m} \frac{\partial^2 \Psi(x)}{\partial x^2} + U(x)\Psi(x) &= i\hbar \frac{\partial \Psi(x)}{\partial t} \\ -\frac{\hbar^2}{2m} \frac{\partial^2 \psi(x)}{\partial x^2} + U(x)\psi(x) - i\hbar \frac{\partial \Psi(x)}{\partial t} &= 0 \end{aligned}$$

Isto sugere que as soluções da equação têm a forma geral:

$$\Psi(x, t) = \psi(x).f(t)$$

Introduzindo-a na **equação de Schrödinger** e rearranjando:

$$\left[ -\frac{\hbar^2}{2m} \frac{d^2\psi(x)}{dx^2} + U(x) \right] \psi(x) - \frac{i\hbar}{f(t)} \frac{df(t)}{dt} = 0$$

Supondo uma variação de  $x$  somente o termo entre parênteses poderia variar, pois o outro termo é independente de  $x$ . Ora como a soma dos dois termos é nula, então ambos são iguais a uma constante que deverá ser a energia total da partícula,  $E$ . De fato, o operador **Hamiltoniano** (presente no termo entre parênteses) representa a energia total, a qual é uma constante  $E$ .

Assim,  $\psi(x)$  é solução da equação:

$$\left[ -\frac{\hbar^2}{2m} \frac{d^2\psi(x)}{dx^2} + U(x) \right] \psi(x) = E\psi(x)$$

que pode ser reescrita como:

$$\left[ -\frac{\hbar^2}{2m} \frac{d^2\psi(x)}{dx^2} + U(x) \right] \psi(x) = E\psi(x)$$

ou  $\hat{H}\psi = E\psi$ , que se designa por **equação de Schrödinger independente do tempo**.

**Definição** (Autofunção)

Vimos que para extrair informações sobre um dado sistema quântico é necessário resolver a equação de **Schrödinger**, cuja solução é uma função de onda ( $\psi$ ). Neste sentido dizemos que  $\psi$  é uma **autofunção do operador Hamiltoniano  $\hat{H}$** , isto é;

$$\hat{H}\psi = E\psi \text{ (equação de autovalor)}$$

As funções de onda  $\psi$  de um sistema são **autofunções** do operador **Hamiltoniano  $\hat{H}$** , sendo os autovalores as energias permitidas  $E$ . Onde  $E$  é a energia que é representada pelo autovalor do operador  $\hat{H}$ . Resumidamente, podemos dizer que a equação de **Schrödinger** é uma equação de *autovalor* da forma:

$$\text{(operador)}(\text{função}) = (\text{fator constante}) \times (\text{mesma função})$$

onde o 'fator constante' é o **autovalor do operador  $\hat{H}$**  e a função (por exemplo,  $\psi$ ) é uma **autofunção**. Veja na Figura 108 como segue:

Então, na prática, na mecânica quântica, estamos sempre procurando por **funções que são autofunções** de um dado operador, especialmente do operador **Hamiltoniano  $\hat{H}$**  usado para se calcular a energia, isto é:

$$\text{(operador Hamiltoniano)}(\text{função de onda}) = (\text{energia}) \times (\text{a mesma função de onda})$$

Este procedimento é aplicável a qualquer observável. Isto significa que os autovalores de um dado operador devem ser números reais, caso contrário eles não



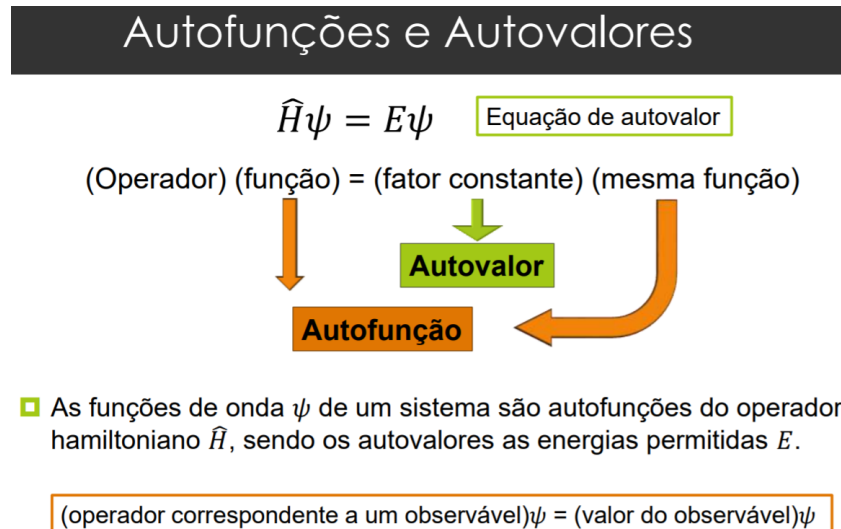


Figura 108 – Operador Hamiltoniano, Autofunções e Autovalores.

Fonte: Postulados da Mecânica Quântica, Química Quântica, Carla Dalmolin, (DALMOLIN, 2010)

representarão observáveis que possam ser medidos em laboratório. Em resumo podemos dizer que as autofunções de um dado operador geram sempre autovalores reais e, portanto são **observáveis**.

## 8.7 Autovalores, Autovetores e Representação Espectral

**Definição** (Autovetor e Autovalor) - Dado um operador linear  $A$  sobre o espaço de Hilbert  $\mathcal{H}_n$ ,  $\lambda \in \mathbb{C}$  e  $\phi \in \mathcal{H}_n$ , se  $A\phi = \lambda\phi$ , então  $\phi$  é um *autovetor* de  $A$  e  $\lambda$  é o *autovalor* associado a  $\phi$ . O *espectro* de  $A$  é o conjunto de todos seus *autovalores*.

Para um dado operador  $A$ , se tivermos  $A\phi = \lambda\phi$  e  $\lambda \in \mathbb{C}$ , então  $A(c\phi) = c(A\phi) = c\lambda\phi = \lambda(c\phi)$  pela linearidade de  $A$ . Logo  $c\phi$  também é um autovetor de  $A$ . Se  $A\phi_1 = \lambda\phi_1$  e  $A\phi_2 = \lambda\phi_2$ , com  $\phi_1 \neq \phi_2$ , segue da mesma forma que  $A(\phi_1 + \phi_2) = \lambda(\phi_1 + \phi_2)$ , de modo que  $\phi_1 + \phi_2$  também é autovetor de  $A$ . Como  $A(0) = \lambda \cdot (0)$ , temos que o conjunto de todos os autovetores associados a  $\lambda$  é um subespaço de  $\mathcal{H}$ , chamado de auto-espaço de  $\mathcal{H}$  e denotado por  $\mathcal{H}_\lambda$ .

Se os autovalores distintos de uma *matriz hermitiana*  $A$  são  $\lambda_1, \dots, \lambda_m$  e a dimensão do autoespaço  $\mathcal{H}_{\lambda_i}$  é  $m(i)$ , então  $\sum_{i=1}^m m(i) = m$ , ou seja, o subespaço gerado por todos os autovetores tem dimensão  $n$ .

**Proposição** O determinante de uma matriz  $A$  é igual ao produto de seus autovalores. Além disso, o *traço* (soma dos elementos da diagonal) de uma matriz  $A$ , denotado por  $Tr(A)$ , é igual à soma dos autovalores de  $A$ .

A prova deste resultado pode ser vista em (TREFETHEN; BAU, 1997).

**Proposição** Todos os autovalores de uma matriz hermitiana  $A$  são reais. Além disso, autovetores de  $A$  correspondendo a autovalores diferentes são ortogonais, ou seja, para  $\lambda_1 \neq \lambda_2$ ,  $\phi_1 \perp \phi_2$

A prova deste resultado pode ser vista em (TREFETHEN; BAU, 1997).

Considere um espaço de **Hilbert**  $\mathcal{H}_n$  e uma matriz hermitiana  $A$  de dimensão  $n$  com autovalores  $\lambda_1, \dots, \lambda_m$  e respectivos autoespaços  $\mathcal{H}_{\lambda_1}, \dots, \mathcal{H}_{\lambda_m}$ . Existe uma base ortonormal  $B_{\lambda_i}$  para cada autoespaço  $\mathcal{H}_{\lambda_i}$ ,  $1 \leq i \leq m$ .

Então  $B = \bigotimes_{i=1}^m B_{\lambda_i}$  é uma base ortonormal de  $\mathcal{H}$ , pelos resultados apresentados acima.

**Teorema 7.17** - (Representação Espectral). Seja  $A$  uma matriz hermitiana e  $\lambda_1, \dots, \lambda_k$  seus autovalores distintos. Então  $A = \sum_{i=1}^k \lambda_i P_i$ , onde  $P_i$  é o projetor sobre o autoespaço correspondente a  $\lambda_i$ .

A prova deste teorema se encontra na seção A.5 em (CARDONHA; SILVA; FERNANDES, 2004)

## 8.8 Produto Tensorial

**Tensores** são entidades geométricas introduzidas na Matemática e na Física para generalizar a noção de escalares, vetores e matrizes. Assim como tais entidades, um *tensor* é uma forma de representação associada a um conjunto de operações tais como a soma e o produto, e que tem a ver com os conceitos de *tensão* e *deformação* e suas respectivas análises de tensão e deformação, muito estudadas nas engenharias mecânica e civil.

Usa-se o termo *tensor* como uma transformação linear de  $\mathcal{V}$  em  $\mathcal{V}$ . Logo, um tensor  $T$  é uma transformação linear que associa a cada vetor  $u$ , um outro vetor  $v$  através da operação

$$v = T(u)$$

Assim para quaisquer  $u, v \in \mathcal{V}$ , tem-se:

- $T(u + v) = T(u) + T(v)$ ,  $\forall u, v \in \mathcal{V}$
- $T(\alpha v) = \alpha T(v)$ ,  $\forall v \in \mathcal{V}, \forall \alpha \in \mathbb{R}$

De forma geral, dados os vetores  $u_1, u_2, \dots, u_n$  e escalares  $\alpha_1, \alpha_2, \dots, \alpha_n$  as relações anteriores podem ser resumidas como:

$$T(\alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_n u_n) = \alpha_1 T(u_1) + \alpha_2 T(u_2) + \dots + \alpha_n T(u_n) = T(\alpha_i u_i) = \alpha_i T(u_i)$$

O conjunto de todos os tensores forma o espaço vetorial, se a adição e a multiplicação por escalar forem definidas ponto a ponto, ou seja,

$(S + T)$  e  $\alpha S$  ( $\alpha \in \mathbb{R}$ ) são os tensores definidos por

- $(S + T)v = S(v) + T(v)$
- $(\alpha S)v = \alpha S(v)$

A forma com a qual se definiu o conceito de *tensor*, acima, permite que se faça uma associação biunívua (um-a-um e inversamente) entre *tensores* e *matrizes*. Dessa maneira, as operações matriciais equivalentes às duas últimas operações tensoriais são, respectivamente, a soma e o produto por escalar usualmente conhecidos do estudo de matrizes.

De um modo mais formal, *tensores* são a generalização dos conceitos de vetor, funcional linear, transformação linear, forma bilinear, e de modo geral, aplicações  $n$ -lineares que levam  $n_1$  vetores a  $n_2$  vetores. *Tensores* são essenciais em diversas áreas da Física, como mecânica clássica, electromagnetismo e a teoria da relatividade.

Assim como os componentes de um vetor mudam quando mudamos a base do espaço vetorial, os componentes de um tensor também mudam sob tal transformação.

Em matemática, o *produto tensorial*, simbolizado por  $\otimes$  em (BOURBAKI, 1989), pode ser aplicado em diferentes contextos a **vetores**, **matrizes**, **espaços vetoriais**, **álgebras**, **espaços vetoriais topológicos**. Em cada caso o significado do símbolo é o mesmo: a **operação bilinear** (forma bilinear) mais geral. Em alguns contextos, este produto é também referido como sendo **produto externo**.

Em matemática, sobretudo na **álgebra linear** e na **análise funcional**, uma **forma bilinear definida em um espaço vetorial** (sobre um corpo  $\mathbb{K}$ ) é uma função  $B : V \times V \rightarrow \mathbb{K}$ , linear em ambas as variáveis.

**Definição 7** - Sejam  $\mathcal{H}_1, \mathcal{H}_2$  espaços de **Hilbert** com respectivas bases ortonormais.

$$\mathbf{B}_1 = \{|\phi_1\rangle, \dots, |\phi_n\rangle\} \text{ e } \mathbf{B}_2 = \{|\psi_1\rangle, \dots, |\psi_n\rangle\}$$

O produto tensorial de  $\mathcal{H}_1$  e  $\mathcal{H}_2$ , denotado por  $\mathcal{H}_1 \otimes \mathcal{H}_2$ , é o espaço de Hilbert  $\mathcal{H}$  gerado pelo conjunto:

$$\mathbf{B} := \mathbf{B}_1 \times \mathbf{B}_2 = \{(|\phi_i\rangle, |\psi_j\rangle) : |\phi_i\rangle \in \mathbf{B}_1, |\psi_j\rangle \in \mathbf{B}_2\}$$

com produto interno entre:

$$(|\phi_i\rangle, |\psi_j\rangle) \text{ e } (|\phi_k\rangle, |\psi_l\rangle)$$

dado por  $\langle \phi_i | \phi_k \rangle, \langle \psi_j | \psi_l \rangle$ , para quaisquer  $\phi_i, \phi_k \in \mathbf{B}_1$  e  $\psi_j, \psi_l \in \mathbf{B}_2$ .

Da definição, os elementos de  $B$  são ortonormais, de forma que  $B$ , o conjunto gerador, é também uma base para  $\mathcal{H}_1 \otimes \mathcal{H}_2$  e, portanto,

$$\dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = \dim \mathcal{H}_1 \dim \mathcal{H}_2$$

O produto interno entre quaisquer elementos de  $\mathcal{H}_\infty \otimes \mathcal{H}_\infty$  é totalmente determinado pelo produto interno entre os elementos dessa base, que foi definido acima.

Definimos o produto tensorial por:

$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=1}^n \sum_{j=1}^m c_i d_j (|\phi_i\rangle, |psi_j\rangle)$$

Algumas vezes será mais conveniente escrevermos  $|\phi\rangle |\psi\rangle$  ou  $|\phi\psi\rangle$  ou  $|\phi\rangle, |\psi\rangle$  no lugar de  $|\phi\rangle \otimes |\psi\rangle$ .

Como observado acima, o produto interno, entre os elementos de  $\mathcal{B}_1$  e  $\mathcal{B}_2$ , determina o produto interno entre quaisquer elementos de  $\mathcal{H}_1 \otimes \mathcal{H}_2$ .

Em particular, pode-se provar facilmente que o produto interno entre  $|\phi\rangle \otimes |\psi\rangle$  e  $|\phi'\rangle \otimes |\psi'\rangle$  é dado por:

$$\langle \phi | \phi' \rangle | \langle \psi | \psi' \rangle$$

para quaisquer  $|\phi\rangle, |\phi'\rangle \in \mathcal{H}_1$  e  $|\psi\rangle, |\psi'\rangle \in \mathcal{H}_2$ .

Seguem as seguintes propriedades do produto tensorial, para quaisquer vetores  $|\phi\rangle \in \mathcal{H}_1, |\psi\rangle \in \mathcal{H}_2, |\gamma\rangle \in \mathcal{H}_3$  e  $c \in \mathbb{C}$  como na Figura 109:

1.  $(|\phi\rangle \otimes |\psi\rangle) \otimes |\gamma\rangle = |\phi\rangle \otimes (|\psi\rangle \otimes |\gamma\rangle)$  (propriedade associativa)
2.  $c(|\phi\rangle \otimes |\psi\rangle) = (c|\phi\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes (c|\psi\rangle)$
3.  $(|\phi\rangle + |\psi\rangle) \otimes |\gamma\rangle = |\phi\rangle \otimes |\gamma\rangle + |\psi\rangle \otimes |\gamma\rangle$  (propriedade distributiva à esquerda)
4.  $|\phi\rangle \otimes (|\psi\rangle + |\gamma\rangle) = |\phi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\gamma\rangle$  (propriedade distributiva à direita)

Figura 109 – Propriedades associativa e distributiva de tensores.

Fonte: (CARDONHA; SILVA; FERNANDES, 2004)

O símbolo  $\otimes$  foi usado nos primórdios pelos **fenícios**, na letra *teth*, mas a moderna notação é presumivelmente uma modificação do sinal de multiplicação  $\times$ .

Sejam  $\mathcal{B}_1, \dots, \mathcal{B}_m$  bases ortonormais dos espaços de **Hilbert**  $\mathcal{H}_1, \dots, \mathcal{H}_m$ .

Então o conjunto,

$$\mathcal{B}_1 \otimes \dots \otimes \mathcal{B}_m = \bigotimes_{i=1}^m \mathcal{B}_i = \{\phi_1 \otimes \dots \otimes \phi_m : \phi_i \in \mathcal{B}_i\}$$

é uma base para o espaço de **Hilbert**.

$$\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_m = \bigotimes_{i=1}^m \mathcal{H}_i$$

**Exemplo:**

Considere o espaço de **Hilbert** bidimensional  $\mathcal{H}^2$  com base  $B^2 = \{|0\rangle, |1\rangle\}$ , onde

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Então o conjunto

$$\bigotimes_{i=1}^n B^2 = \{|x_1\rangle \otimes \dots \otimes |x_n\rangle : x_1, \dots, x_n \in \{0, 1\}^n\}$$

é uma base ortogonal do espaço de **Hilbert**

$$\mathcal{H}_{2^n} = \bigotimes_{i=1}^n \mathcal{H}^2$$

de dimensão  $2^n$ .

Estendendo o produto tensorial para matrizes correspondentes a operadores lineares.

Considere as matrizes:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}$$

O produto tensorial de A e B, denotado por  $A \otimes B$  é definido por

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}$$

Seguem as seguintes propriedades na Figura 110:

1.  $(A \otimes B)(|\phi\rangle \otimes |\psi\rangle) = (A|\phi\rangle) \otimes (B|\psi\rangle)$
2.  $(A \otimes B)(C \otimes D) = AC \otimes BD$
3.  $(A \otimes B)^* = A^* \otimes B^*$ .

Figura 110 – Propriedades algébricas para matrizes-tensores em espaço de matrizes.

Fonte: Apêndice A, seção A.6 em (CARDONHA; SILVA; FERNANDES, 2004)

## 8.9 Bibliografia e Fonte de Consulta

Computação Quântica - <[www.tecmundo.com.br/computacao\\_quantica/](http://www.tecmundo.com.br/computacao_quantica/)>

A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N.H. Margolus, P.W. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457-3467, 1995.

R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci.*, 454(1969):339-354, 1998.

D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London Ser. A*, 400(1818):97-117, 1985.

A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.*, 68(3), 1996.

E. Prugovecki. *Quantum Mechanics in Hilbert Space*, volume 92 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, second edition, 1981.

E. Rieffel and W. Polak. Introduction to quantum computing. *ACM Computing Surveys*, 32(3):300-335, 2000.

Carlos H. Cardonha, Marcel K. de Carli Silva, Cristina G. Fernandes. *Computação Quântica: Complexidade e Algoritmos*. Departamento de Ciência da Computação, Universidade de São Paulo. Iniciação Científica: Agosto/2003 a Dezembro/2004.

P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124-134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

P.W. Shor. 140 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484-1509, 1997.

D.R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474-1483, 1997.

## 8.10 Para saber mais - Leitura Recomendada

D. Deutsch. Quantum computational networks. *Proc. Roy. Soc. London Ser. A*, 425(1868):73-90, 1989.

Movimento Browniano - <[https://www.fisica.net/mecanica-quantica/movimento\\_browniano.pdf](https://www.fisica.net/mecanica-quantica/movimento_browniano.pdf)>



## Parte III

# A Computação Quântica





## Da Mecânica Quântica à Computação Quântica

Estritamente falando, a formulação algébrica da mecânica quântica (**Hilbert**), introduzida nos capítulos anteriores, não é uma teoria física, mas em vez disso, fornece uma estrutura para formular teorias físicas no contexto quântico. Dependendo sobre como exatamente os espaços de **Hilbert** (aqui nos interessa espaços de **Hilbert** que descrevem os estados de um sistema quântico) são construídos, surgem teorias diferentes. A **computação quântica** é mais uma teoria sobre o formalismo mecânico quântico abstrato, construída em conceitos como *qubits* e *portas quânticas*, independentemente do modelo físico subjacente.

Esta abordagem de cima para baixo é, ao mesmo tempo, a maior força e a maior fraqueza da computação quântica. Embora garanta que o modelo computacional é de fato o mais geral, que é fisicamente realizável, num universo mecânico quântico, a falta de uma concreta e escalável "implementação de referência", como a máquina **Turing** é para computação clássica, deixa a questão de saber, se os computadores quânticos, com mais de um punhado de qubits, são de fato possíveis, sob pressupostos realistas de precisão experimental.

### 9.1 Além da tese de Church-Turing

Em 1936, **Alan Turing** formalizou conceito do que é computável, construindo um dispositivo abstrato, chamado máquina de **Turing**, que ele provou ser capaz de realizar qualquer computação efetiva (isto é, mecânica, algorítmica). Na mesma época, **Alonzo Church** mostrou que qualquer função de inteiros positivos é efetivamente *calculável*, somente se for *recursiva*. Ambas as descobertas são, na verdade, equivalentes e são comumente referidas como a *Tese de Church-Turing*. Na sua forma forte, pode ser resumida como:

*Qualquer processo algorítmico pode ser simulado eficientemente usando uma máquina de **Turing**.*

Isso significa que, independentemente do tipo de máquina que realmente é usada para uma determinada computação, pode ser encontrada uma máquina **Turing**

equivalente que resolve o mesmo problema com apenas o custo polinomial.

A Tese da Church-Turing foi atacada quando, em 1977, **Robert Solovay** e **Volker Strassen** publicaram um teste rápido de Monte-Carlo para a primalidade (SOLOVAY; STRASSEN, 1977), (NIELSEN; CHUANG, 2000), um problema para o qual nenhum algoritmo determinístico eficiente era conhecido naquele tempo <sup>1</sup> (AGRAWAL; KAYAL; SAXENA, 2004). Embora este desafio possa ser facilmente resolvido usando uma máquina de **Turing** probabilística, levanta a questão, se ainda existem modelos de computação mais poderosos.

Em 1985, **David Deutsch** (1953-), um professor visitante de Física no *Centre for Quantum Computation* no *Clarendon Laboratory, Oxford University*, adotou uma abordagem mais geral e tentou desenvolver uma máquina abstrata, o *Universal Quantum Computer*, que é não visando alguma noção formal de computação, mas deveria ser capaz de efetivamente simular um sistema físico arbitrário e, conseqüentemente, qualquer dispositivo computacional realizável (DEUTSCH, 1985), (SVOZIL, 1996). **Deutsch** também descreveu um simples algoritmo quântico que seria capaz de determinar em um único passo, se uma determinada função  $f : \mathbf{B} \rightarrow \mathbf{B}$  (uma função de previsão) é ou constante ou balanceada. O algoritmo foi posteriormente generalizado para funções de  $n$  bits  $f : \mathbf{B}^n \rightarrow \mathbf{B}$  (Problema Deutsch-Jozsa (DEUTSCH; JOZSA, 1992)) e demonstra que um computador quântico é, de fato, mais poderoso do que uma máquina **Turing**-probabilística.



Figura 111 – David Deutsch - O Universal Quantum Computer e seu simples algoritmo quântico.

Fonte: <<https://www.daviddeutsch.org.uk>>

Ao mesmo tempo, 1985, **Richard Feynman** (1918-1988) foi um físico norte-americano do século XX, um dos pioneiros da *eletrodinâmica quântica* e Nobel de Física de 1965. Ele, também, mostrou como *Hamiltonianos locais* (um campo **Hamiltoniano**, em coordenadas locais, define um sistema de equações diferenciais ordinárias (ALMEIDA, 2012), que pode ser construído para realizar cálculos clássicos arbitrários (FEYNMAN, 1985). Em 1994, **Peter Shor** demonstrou como a *fatoração* primária

<sup>1</sup> In 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena encontraram um teste determinístico de primalidade <[https://en.wikipedia.org/wiki/AKS\\_primality\\_test](https://en.wikipedia.org/wiki/AKS_primality_test)> e (CARDONHA; SILVA; FERNANDES, 2004) (Apêndice D) com um pior caso de tempo na complexidade  $O(n^{12})$ .

e o cálculo do *logaritmo discreto* podiam ser eficientemente realizados em um computador quântico (SHOR, 1994a) (SHOR, 1994b). A imensa importância prática desses problemas para a criptografia, tornou o algoritmo de **Shor**, uma aplicação da computação quântica, relevante.

Um ano depois, **Lov Kumar Grover** (1961-), um cientista indiano da ciência da computação, originou o algoritmo de busca em uma base de dados, usado na computação quântica. Ele é o inventor do que foi provado ser o mais rápido possível algoritmo de busca que pode ser executado em um computador quântico.

**Peter Zoller** (1952-) é um físico austríaco. Ele trabalha com óptica quântica e teoria da informação quântica, conhecido principalmente por seu trabalho pioneiro sobre computador quântico e também pela conexão entre óptica quântica e física do estado sólido. **Juan Ignacio Cirac Sasturain** (1965-), conhecido por **Ignacio Cirac**, é um físico espanhol. É diretor da seção *Theorie* no Instituto Max Planck de Óptica Quântica, em *Garching bei München*. Naquele momento, **Peter Zoller** e **Ignacio Cirac** demonstraram como uma *linear ion trap* (armadilha de íons) podia ser usada para armazenar *qubits* e executar cálculos quânticos (CIRAC; ZOLLER, 1995). Ver em: <[http://www.mpq.mpg.de/cms/mpq/people/Cirac\\_Ignacio.shtml](http://www.mpq.mpg.de/cms/mpq/people/Cirac_Ignacio.shtml)>

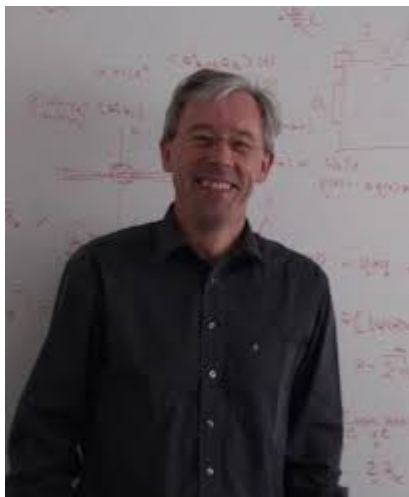


Figura 112 – Peter Zoller - O trabalho pioneiro sobre computador quântico.

Fonte: <<https://iqoqi.at/en/zoller-gruppe>>

Na teoria da complexidade computacional e em computação quântica, o algoritmo de **Shor** <[https://pt.wikipedia.org/wiki/Algoritmo\\_de\\_Shor](https://pt.wikipedia.org/wiki/Algoritmo_de_Shor)>, batizado em homenagem ao matemático **Peter Shor** (1959-) 114, é um algoritmo quântico (NIELSEN; CHUANG, 2000) (MOSCA, 2008) para fatorar um número  $N$  não primo de  $L$  bits. Em 2001, uma equipe da IBM conseguiu implementar o *algoritmo de Shor* sobre um computador quântico *NMR 7-qubit* para fatorar o número 15 (CHUANG, 2001).

## 9.2 A necessidade da Computação Quântica

A computação quântica é a ciência que estuda as aplicações das teorias e propriedades da mecânica quântica na Ciência da Computação. Dessa forma seu principal foco é o desenvolvimento do computador quântico.



Figura 113 – Ignacio Cirac - A pesquisa para armazenar *qubits* e executar cálculos quânticos.

Fonte: <[https://en.wikipedia.org/wiki/Juan\\_Ignacio\\_Cirac\\_Sasturain](https://en.wikipedia.org/wiki/Juan_Ignacio_Cirac_Sasturain)>



Figura 114 – Peter Shor - Aos 35 anos, quando criou o algoritmo quântico para fatorar inteiros.

Fonte: <[https://pt.wikipedia.org/wiki/Peter\\_Shor](https://pt.wikipedia.org/wiki/Peter_Shor)>

Na computação clássica o computador é baseado na arquitetura de **John von Neumann**, que faz uma distinção clara entre elementos de processamento e armazenamento de dados, isto é, possui processador e memória interligados por um barramento de comunicação, sendo seu processamento sequencial.

Entretanto os computadores atuais possuem limitações, como por exemplo na área de Inteligência Artificial (IA) onde não existem computadores com potência ou velocidade de processamento suficiente para suportar uma IA avançada. Dessa forma surgiu a necessidade da criação de um computador alternativo dos usuais que resolvesse problemas de IA, ou outros como a fatoração em primos de números muito grandes, logaritmos discretos e simulação de problemas da Física Quântica.

A **Lei de Moore** afirma que a velocidade de um computador é dobrada a cada 18 meses. Em 1965, **Gordon Moore** estabelece uma lei que diz que o número de transistores usados em um circuito integrado dobra a cada dois anos. Assim sempre houve um crescimento constante na velocidade de processamento dos computadores. Entretanto essa evolução pode atingir um certo limite, um ponto onde não será possível aumentar essa velocidade, e então se fez necessário uma revolução significativa na computação para que este obstáculo fosse quebrado. Com a constante miniaturização dos chips cogitou-se que tecnologia convencional utilizada para a sua fabricação esbarraria nas dificuldades impostas pela redução do tamanho dos componentes. Os **efeitos quânticos começam a interferir no funcionamento dos componentes à medida que eles diminuem**. Uma possível solução: **um novo paradigma da computação, usando a mecânica quântica para fazer computação**. E assim as pesquisas em Computação Quântica se tornaram muito importantes e a necessidade do desenvolvimento de uma máquina extremamente eficiente se torna ainda maior.

### 9.3 O que é Computação Quântica?

Velocidade de processamento exponencialmente maior do que o mais avançado computador atual: isso é uma das vantagens que se espera do sistema computacional baseado nos conceitos da mecânica quântica: o computador quântico. A computação quântica é fundamentada em conceitos criados pela Física quântica como o da *sobreposição* (quando uma partícula está em diferentes condições contraditórias simultaneamente) e do *entrelaçamento* (quando a alteração em uma partícula provoca o mesmo efeito em outra que se encontra distante). Os grandes trunfos da Computação Quântica são a **sobreposição/superposição** e o **emaranhamento/entrelaçamento**.

**Qubits e espaços de Hilbert** - Um *qubit* é um sistema quântico com dois estados. Os *qubits* "moram" em um espaço de **Hilbert**, que é um **espaço vetorial completo** sobre  $\mathbb{C}$  munido de *produto interno*. Em um *espaço de Hilbert*, uma porta lógica quântica é uma transformação linear unitária (i.e., que preserva a norma dos vetores). Além disso, consequências do produto tensorial em espaços de **Hilbert** - *Não-Clonagem*: é impossível copiar estados superpostos usando um circuito quântico; *Reversibilidade*: é possível voltar a alguma configuração anterior em um processamento ("desapagar"); *Caracterização de estados emaranhados*; *Algoritmos quânticos*.

**John von Neumann** formalizou os conceitos da computação quântica no contexto de um espaço de **Hilbert**. Os resultados deste capítulo estão no contexto dos espaços de **Hilbert** aplicados à computação quântica. A principal referência para esse capítulo é (NIELSEN; CHUANG, 2010).

## 9.4 O qubit e suas propriedades

Podemos fazer uma representação bastante simplória de um *qubit* (bit quântico) utilizando uma moeda. Para esse fim, representaremos o resultado 'cara' com o '0' e o resultado 'coroa' com o '1'. Conforme intuímos, as moedas são objetos macroscópicos, governados pela física clássica, e por isso ao lançarmos a moeda (girarmos como se roda um peão) só obtemos um dos resultados ('0' ou '1') em cada jogada (MATIELLO et al., 2012).

No entanto, se a moeda se comportasse como os *objetos microscópicos*, que obedecem os *princípios da mecânica quântica*, teríamos que as faces 'cara' e 'coroa' poderiam ser vistas ao mesmo tempo, ou seja, no lançamento de uma moeda, o resultado cara e coroa coexistiriam. Esse resultado é possível graças a uma das propriedades da mecânica quântica, denominada de *sobreposição* (*superposição*). Se novamente supusermos que uma moeda é um objeto quântico, os resultados '1' e '0' são denominados de estados básicos (fundamentais) e são representados por  $|1\rangle$  e  $|0\rangle$ , respectivamente, e, nesse caminho, um estado quântico genérico desse *qubit* é representado por meio da expressão abaixo:

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

onde  $\alpha$  e  $\beta$  são números complexos, associados às probabilidades de se encontrar, no lançamento de uma moeda  $|0\rangle$  e  $|1\rangle$ , respectivamente. A *superposição de estados*, apesar de parecer um pouco estranha, pode ser entendida mediante este exemplo, que trata de uma forma simples de analisar o princípio da superposição das soluções da equação de **Schroedinger** (FEYNMAN, 1982a) (PIZA, 2003) (FREIRE; PESSOA; BROMBERG, 2010) (SAKURAI, 1994). Tal princípio afirma que, se para um determinado problema, a equação de **Schroedinger** admitir duas soluções distintas  $|a\rangle$  e  $|b\rangle$ , então o sistema pode ser descrito por meio da superposição das duas soluções, o que é matematicamente escrito como (EISBERG; RESNICK, 1979b) (COHEN-TANNOUDJI; DIU; LALOE, 1992).

$$|\varphi\rangle = |a\rangle + |b\rangle \text{ (o sinal de '+' significa **sobreposição**)}$$

onde os estados  $|a\rangle$  e  $|b\rangle$  existem simultaneamente. Contudo, quando observarmos o sistema, ou seja, quando efetuarmos uma medição, um dos estados **colapsa** (deixa de existir) e o outro (o de maior probabilidade) é então detectado. Nesse sentido, o exemplo da moeda faz alusão a essa curiosa propriedade quântica de superposição.

Agora, se pensarmos nos bits 0 e 1, teremos, para a computação quântica, os estados quânticos correspondentes para representar os bits clássicos 0 e 1 e, portanto, o chamaremos *qubit*. Os valores 0 e 1 que um bit clássico pode assumir serão substituídos pelos vetores  $|0\rangle$  e  $|1\rangle$  representados por dois vetores do espaço de Hilbert 2-dimensional de números complexos  $\mathbb{C}$ , com produto interno, tais como:

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

**Definição** (Vetores unitários)

Os vetores  $|0\rangle$  e  $|1\rangle$  formam uma *base ortonormal* (vetores ortogonais e unitários) do espaço  $\mathbb{C}^2$ , que define uma **base computacional**.

Agora podemos ter um *qubit* genérico  $|\varphi\rangle$  resultado da combinação linear dos estados  $|0\rangle$  e  $|1\rangle$

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

onde  $\alpha$  e  $\beta$  são dois números complexos representando amplitudes de probabilidades dos estados quânticos  $|0\rangle$  ou  $|1\rangle$  virem a ocorrer, quando uma **medida** for tomada para se obter um resultado quântico.

$|\varphi\rangle$  é chamado de **superposição/sobreposição** dos vetores da base com amplitudes  $\alpha$  e  $\beta$ .

$|\varphi\rangle$  está **simultaneamente** nos estados  $|0\rangle$  e  $|1\rangle$ .

Nessa perspectiva, um *qubit* pode existir **num estado contínuo** entre  $|0\rangle$  e  $|1\rangle$ , até que ele seja observado (medido). Uma evolução temporal atua no nível quântico, mas não temos acesso a essa! Podemos imaginar uma "quantidade de informação infinita" armazenada em  $|\varphi\rangle$ . **Essa informação está no mundo quântico**. Como fazer para aproveitarmos toda essa informação armazenada em um *qubit*? Precisamos trazê-la ao mundo clássico. E para trazê-la ao mundo clássico precisamos fazer uma **medida**. A **medida** faz a ligação entre o mundo quântico e o mundo clássico!

A única forma de averiguar o que "realmente" aconteceu com a moeda será realizar uma **medida**, interagindo com a moeda e observando o resultado. Em alguns casos encontraremos a moeda em  $|0\rangle$  e em outros em  $|1\rangle$ . Isso ocorre porque ao realizar a medida, o observador interage com o sistema e o altera. A medida altera o estado do qubit, rompendo a superposição dos dois estados, fazendo com o que o sistema seja observado em um dos dois estados possíveis (**o de maior probabilidade**). E isso é uma forma simplista de explicar o que chamamos de **colapso de estados quânticos** (ou colapso da função de onda), que é uma característica inerente ao processo de medição em mecânica quântica. E então, quando um *qubit* é observado (medido), o resultado será sempre  $|0\rangle$  ou  $|1\rangle$ , probabilisticamente, ou seja, imaginando-se as probabilidades da ocorrência dos estados base  $|0\rangle$  ou  $|1\rangle$  teremos então:

- $|0\rangle$  com probabilidade  $|\alpha|^2$ ; ou
- $|1\rangle$  com probabilidade  $|\beta|^2$ .

$\alpha$  e  $\beta$  não podem ser conhecidos através de uma medida. Além disso,  $|\alpha|^2 + |\beta|^2 = 1$ .

Não é possível calcular exatamente os valores de  $|\alpha|$  e  $|\beta|$  mesmo que tenhamos um grande número de estados  $|\varphi\rangle$  iguais. Mesmo após repetidas medidas só teríamos os resultados  $|0\rangle$  ou  $|1\rangle$ . Mesmo com a quantidade infinita deles, isso só leva a um valor aproximado desses coeficientes pois correspondem apenas a probabilidades  $|\alpha|^2$  e  $|\beta|^2$  (PORTUGAL et al., 2004).



Tanto sacrifício para se saber o valor de um único *qubit*!!

Mesmo que um bit quântico possa ser colocado em *infinitos estados de superposição*, é apenas possível extrair um único bit de informação clássica de um único bit quântico. A razão pela qual não é possível obter mais informações de um *qubit* do que de um bit clássico é que essa informação só pode ser obtida por **medição**. E quando um *qubit* é medido, a medição muda o estado para um dos estados básicos. Experimente rodar uma moeda e interagir para a parada dela. Como cada medição pode resultar em apenas um dos dois estados quânticos, existem apenas dois resultados possíveis, sendo o resultado associado a um dos vetores da base, dado pelo dispositivo de medição, exatamente como no caso clássico. Paradoxal! Apesar de toda informação contida em um *qubit* só temos acesso a 2 valores!! E agora? (OLIVEIRA; PORTUGAL, 2008)

Temos ainda, um outro fenômeno que ocorre com um estado quântico. **A mecânica quântica nos diz que a evolução temporal de um sistema quântico isolado é descrita matematicamente por uma transformação linear**, mais especificamente, como estamos tratando de vetores-base unitários, teremos então as transformações unitárias:

$$U^\dagger U = U U^\dagger = \mathbb{I}, \text{ onde } U^\dagger = (U^*)^T \text{ (matriz transposta conjugada) (PORTUGAL et al., 2004)}$$

Resumindo: temos, então, **duas interações básicas de um computador quântico com os dados de entrada**: (a) **transformação unitária** e (b) **medida**. A primeira, atuando no nível quântico, e a segunda, fazendo a ligação entre o mundo quântico e o clássico.

Como **a medição muda o estado**, não se pode medir o estado de um *qubit* em duas bases diferentes. Além disso, estados quânticos não podem ser **clonados**, então não é possível medir um *qubit* de duas maneiras, mesmo indiretamente, digamos, copiando o *qubit* e medindo a cópia em uma base diferente da original (RIEFFEL; POLAK, 2000).

Vale destacar, aqui, que os *qubits* são objetos matemáticos com certas propriedades específicas que podem ser implementados como objetos físicos reais. Alguns exemplos de sistemas físicos que podem ser utilizados em computadores quânticos para representar *qubits* são os seguintes: as polarizações diferentes de um fóton; o alinhamento de um spin nuclear em um campo magnético uniforme; e os dois estados de um elétron orbitando ao redor do núcleo de um átomo.

O paradoxo do *qubit* é que ele parece conter uma quantidade infinita de informação, uma vez que seu estado é representado por dois graus contínuos de liberdade. Entretanto, esta conclusão é infundada, devido a uma propriedade adicional e extremamente importante de sistemas quânticos. (OLIVEIRA; PORTUGAL, 2008) Quando um *qubit* é medido, apenas um de dois resultados são obtidos: ou zero ou um. Uma medição de  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  resultará em 0 com probabilidade  $|\alpha|^2$ , levando ao estado  $|\psi'\rangle = |0\rangle$ , ou em 1 com probabilidade  $|\beta|^2$ , levando ao estado  $|\psi'\rangle = |1\rangle$ . Nota-se que o **estado pós medição** do sistema é um novo estado, que é consistente com o resultado da medição. Assim, de uma única medição, obtém-se apenas um único bit de informação sobre  $\alpha$  e  $\beta$  - e o paradoxo está resolvido. Apenas se infinitamente muitos *qubits* preparados identicamente fossem medidos seria possível obter

$\alpha$  e  $\beta$  completamente. Então, em certo sentido, um *qubit* contém grande quantidade de "informação escondida", ou seja, enquanto ele não é medido (ele se encontra em estado de sobreposição dos estados-bases). Esta é uma parte importante do que será explorado na computação quântica, como será visto adiante, considerando as propriedades para múltiplos qubits (MATIELLO et al., 2012). Apesar da estranheza, *qubits* são decididamente reais, sua existência e comportamento foram extensivamente validados por experimentos, e alguns sistemas físicos podem ser usados para se concretizar *qubits*. É possível realizar *qubits* através de duas diferentes polarizações de um fóton; do alinhamento de *spin* nuclear num campo magnético uniforme; ou até de dois estados de um elétron orbitando um átomo, como no nosso exemplo (RIEFFEL; POLAK, 2000).

A **sobreposição quântica** é um dos princípios fundamentais da mecânica quântica. O princípio afirma que estados quânticos válidos podem ser unidos e o resultado será um outro estado quântico válido. Entretanto da mesma maneira que a **sobreposição** de estados permite a criação do computador quântico é essa mesma propriedade que dificulta a construção desses estados. A *sobreposição* é muito sensível a qualquer *micro ruído eletromagnético* que pode alterar o estado do *qubit* fazendo com que a informação que ele continha seja perdida.

É difícil imaginar a sobreposição quântica, porque tendemos a imaginar as "partículas" subatômicas como objetos materiais no sentido tradicional do termo, como se fossem minúsculas bolinhas de bilhar coloridas voando pelo espaço ou ao redor de átomos. De fato a teoria não permite acessar esse nível de detalhe. Mecânica quântica é uma teoria que leva a um tipo de descrição probabilística ondulatória das partículas e sabemos que duas ondas podem superpor-se - vemos nas ondas do mar que se sobrepõem. No caso das "partículas quânticas", essa capacidade das ondas de se superpor se manifesta como a possibilidade de se combinar estados físicos distintos.

Suponhamos agora que temos dois *qubits*. Se estivéssemos trabalhando com a computação clássica, teríamos quatro estados possíveis: 00, 01, 10 e 11. Como consequência, temos que um sistema de dois *qubits* possui quatro estados na base computacional:  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  e  $|11\rangle$ . Contudo, de acordo com o princípio da superposição, exemplificado por **Schrödinger**, um par de *qubits* também pode existir em superposições desses estados, ou seja, temos o seguinte estado

$$|\varphi\rangle = \alpha |00\rangle + \beta |01\rangle + \chi |10\rangle + \delta |11\rangle$$

onde os coeficientes  $\alpha$ ,  $\beta$ ,  $\chi$  e  $\delta$  são números complexos, sendo úteis nos cálculos de probabilidades. Na essência, um computador quântico manipula a informação, como se os quatro estados de dois qubits existissem ao mesmo tempo, e essa propriedade tornaria possível uma capacidade computacional muito além da que temos acesso na atualidade.

Se quisermos tratar de sistemas computacionais quânticos com **mais de um qubit** temos que introduzir o conceito de **produto tensorial** definido num espaço de **Hilbert**. Sejam dois estados:

$$|\varphi\rangle = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_n \end{pmatrix} \text{ e } |\gamma\rangle = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix}$$

O **produto tensorial** entre eles resultará no vetor  $|\chi\rangle = |\varphi\rangle \otimes |\gamma\rangle$  com  $m \times p$  linhas.

### 9.4.1 Estados quânticos

O estado de um sistema físico quântico composto de vários qubits é expresso pelo **produto tensorial dos vetores que representam cada qubit individualmente**.

Supondo os vetores  $P$  e  $Q$  como seguem:

$$P = \begin{pmatrix} a \\ b \end{pmatrix} \quad Q = \begin{pmatrix} c \\ d \end{pmatrix}$$

É necessário compreender a *operação do produto tensorial* para facilitar a compreensão dos *circuitos quânticos*, na construção de *algoritmos quânticos*. O *produto tensorial* é apenas o produto de cada elemento do vetor  $P$  por todos os elementos do vetor  $Q$ .

Assim, os *qubits* são representados por vetores, **operações unitárias** são representadas por matrizes, que também são passíveis de aplicação de produto tensorial.

Supondo as matrizes  $P$  e  $Q$ :

$$P = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \text{ e } Q = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

o produto tensorial entre  $P$  e  $Q$  é apresentado como:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{12} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ a_{21} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{22} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \end{pmatrix}$$

Figura 115 – Produto Tensorial entre P e Q.

Fonte: Feitosa, S., Uma Linguagem de Programação Quântica Orientada a Objeto, Cap.2, Eq.2.5

onde o resultado do produto tensorial entre as matrizes  $P$  e  $Q$  é dado como segue:

É necessário entender a operação **produto tensorial**, para facilitar a compreensão dos **algoritmos** vistos pelos **circuitos quânticos**.

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

Figura 116 – Produto Tensorial entre P e Q.

Fonte: (Feitosa, S., Uma Linguagem de Programação Quântica Orientada a Objeto ..., Cap.2.)

### 9.4.2 Observáveis e medições

Esta subseção está baseada em (CARDONHA; SILVA; FERNANDES, 2004). Informalmente, um *observável* é uma propriedade de um sistema quântico que pode ser medida. Formalmente, definimos um observável  $O$  como um **operador auto-adjunto** em  $\mathcal{H}$ .

Considere a representação espectral de  $O$ , dada em ((CARDONHA; SILVA; FERNANDES, 2004) (Anexo A.17). De acordo com o teorema A.17 em (CARDONHA; SILVA; FERNANDES, 2004) da representação espectral, todo observável  $O$  pode ser escrito como:

$$O = \sum_{\lambda \in \Lambda} \lambda \cdot P_{\lambda}$$

onde  $\Lambda$  é o espectro de  $O$  e, para  $\lambda \in \Lambda$ ,  $P_{\lambda}$  é o projetor sobre  $W_{\lambda}$ , o autoespaço associado a  $\lambda$ . A proposição A.16 em (CARDONHA; SILVA; FERNANDES, 2004) nos garante que os autoespaços de  $O$  são ortogonais, de modo que  $\mathcal{H} = \bigoplus_{\lambda \in \Lambda} W_{\lambda}$ . Algumas vezes será mais conveniente representarmos um *observável* pelo seu **conjunto de autoespaços**. Nesta representação, o observável  $O$  seria dado por:  $\{W_{\lambda} : \lambda \in \Lambda\}$ .

Na mecânica quântica, medições são fundamentalmente diferentes de medições na Física clássica: uma medição altera irreversivelmente o estado quântico observado. Além disso, o resultado das medições é probabilístico.

Medições são feitas relativas a algum observável  $O$ . O resultado numérico de uma medição com relação a um observável  $O$  é um *autovalor* de  $O$ .

## 9.5 Os Fundamentos da Computação Quântica

Nas subseções seguintes, os conceitos que fundamentam a origem da computação quântica são destacados.

### 9.5.1 Diferenciando estados quânticos

Por que um computador quântico poderia, em tese, realizar em minutos, cálculos que nem em bilhões de anos os mais potentes supercomputadores conseguiriam fazer?

Para entendermos a diferença que há entre o mundo clássico e o quântico, para entendermos porque um gato não pode estar em dois lugares, mas **os átomos podem**,

acho que temos de ser capazes de discriminar (diferenciar) os estados. Podemos começar com as seguintes explicações.

Um bit clássico (**bit**) é um sistema de dois estados: 0 ou 1. E esses estados correspondem a valores diferentes em tempos diferentes, definido como a menor unidade em que a informação pode ser codificada, armazenada e transmitida nos computadores atuais e nos sistemas de telecomunicações, como fibras ópticas ou redes sem fio. Num dado momento, um bit clássico, também denominado dígito binário, só pode se encontrar em apenas um de dois valores ou estados possíveis: 0 ou 1, por exemplo. Nos computadores de hoje em dia o 0 é representado pela interrupção da voltagem num circuito (estado *off*) e o 1 pela liberação da corrente (estado *on*).

O **qubit** é o análogo quântico do **bit** clássico. Há, no entanto, diferenças significativas entre os dois conceitos.

Um bit quântico "qubit" é um sistema de três estados: **0** ou **1** e, podem assumir estes dois valores simultaneamente, considerando o princípio da superposição quântica. Veja a Figura 117. (PIVETTA, 2012)

## A diferença entre bit e qubit



Figura 117 – A diferença entre um bit e um qubit.

Fonte: <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>

### 9.5.2 O Princípio da Superposição

Agora, considere um registrador composto por **dois bits clássicos**. Qualquer registrador clássico pode armazenar, em um determinado momento, apenas um em cada quatro números diferentes, ou seja, **o registrador pode estar em apenas uma das quatro configurações possíveis**, como 00, 01, 10, 11.

Entretanto, um registrador quântico composto por **dois qubits** pode armazenar em um dado momento, **ao mesmo tempo**, os quatro números 00, 01, 10, 11, considerando-se o **princípio da superposição quântica**.

Agora, considere um registrador composto por três bits clássicos. Qualquer registrador clássico pode armazenar, em um determinado momento, apenas um, de

oito números diferentes, ou seja, **o registrador pode estar em apenas uma das oito configurações possíveis**, como 000, 001, 010, 011, 100, 101, 110, 111.

Um registrador quântico composto por **três qubits** pode armazenar em um dado momento, **ao mesmo tempo**, os oito números 000, 001, 010, 011, 100, 101, 110, 111, considerando-se o princípio da superposição quântica (118). Isto é bastante notável que todos os oito números estão fisicamente presentes no registrador, mas não deve ser mais surpreendente do que 1 qubit estando em ambos os estados 0 e 1, **ao mesmo tempo**. Como mostra a Figura 118.

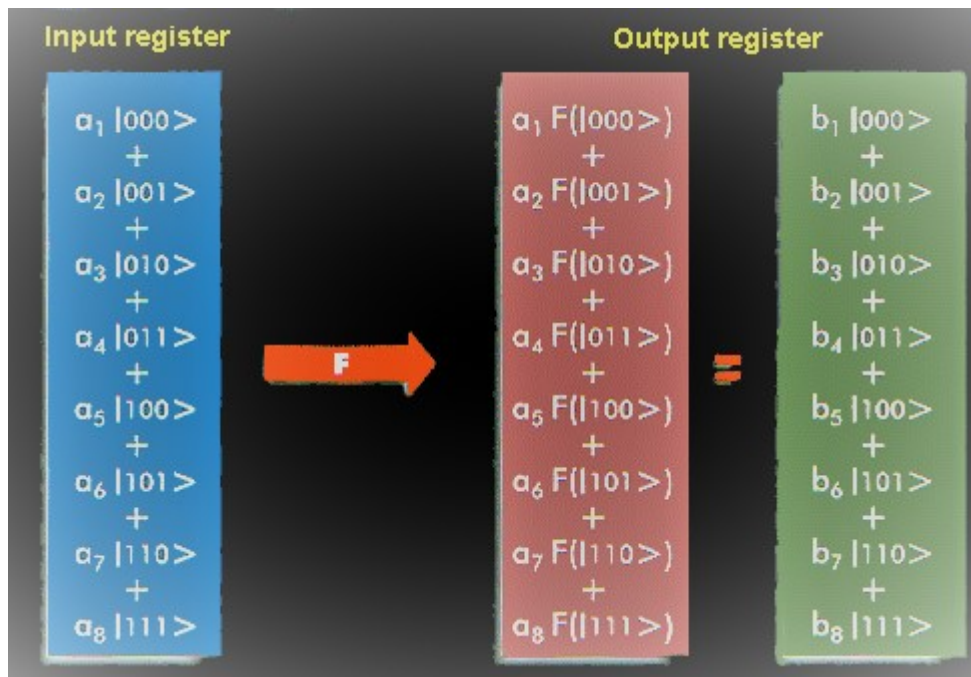


Figura 118 – Ilustração do Princípio da Superposição.

Fonte: <<http://cyber.sibsutis.ru:82/FIONOV/QC/....htm>>

Um computador clássico com três bits de memória pode apenas armazenar dois estados lógicos (uns ou zeros). Num determinado momento, pode conter os bits "000" ou "001" ou "010" ou "011" ou "100" ou "101" ou "110" ou "111". Um computador quântico pode atualmente armazenar 16 valores analógicos em pares para formar 8 números complexos. Em um dado instante, ele poderia conter isto, como na Figura 119:

A primeira coluna mostra todos os estados possíveis para os três bits. Um computador clássico apenas suporta um destes padrões de cada vez. Um computador quântico pode colocar-se na superposição de assumir os 8 estados simultaneamente. A segunda coluna mostra a "amplitude" para cada um dos 8 estados. Estes 8 números complexos são uma imagem dos conteúdos de um computador quântico num determinado momento. Durante a computação, estes 8 números irão modificar e interagir uns com os outros. Neste sentido, um computador quântico de 3-qubit tem muito mais memória do que um computador clássico de 3-bit. No entanto, não existe nenhuma forma de vermos diretamente estes 8 números. Quando o algoritmo é terminado, é feita uma única medida. A medida fornece uma simples linha de 3-bit, e elimina todos os 8 números complexos. A linha fornecida é gerada aleatoriamente.

Estado	Amplitude	Probabilidade
*	(a+ib)	(a <sup>2</sup> +b <sup>2</sup> )
000	0.37 + i 0.04	0.14
001	0.11 + i 0.18	0.04
010	0.09 + i 0.31	0.10
011	0.30 + i 0.30	0.18
100	0.35 + i 0.43	0.31
101	0.40 + i 0.01	0.16
110	0.09 + i 0.12	0.02
111	0.15 + i 0.16	0.05

Figura 119 – Um computador quântico de 3 qubits.

Fonte: <[https://pt.wikipedia.org/wiki/Computador\\_quântico](https://pt.wikipedia.org/wiki/Computador_quântico)>

A terceira coluna da tabela calcula a probabilidade de cada linha possível. Neste exemplo, há uma probabilidade de 14% de que a linha fornecida seja "000", uma de 4% de que seja "001", e assim por diante. Cada probabilidade é encontrada com a execução do quadrado do módulo do número complexo (ou a multiplicação do complexo pelo seu conjugado - dá no mesmo). O quadrado do módulo de  $(a + i.b)$  é  $(a^2 + b^2)$ . As 8 probabilidades somam até 1.

Geralmente, um algoritmo num computador quântico irá dar início a todos os números complexos de modo a se equivalerem a valores, por isso todos os estados terão probabilidades equivalentes. A lista de números complexos pode ser vista como um vector de 8 elementos. Em cada passo do algoritmo, esse vector é modificado ao multiplicá-lo por uma matriz. A matriz advém da física da própria máquina, e será sempre invertível, e irá garantir que as probabilidades continuem a somar até 1 (ou seja, a matriz será sempre ortogonal).

Se continuarmos adicionando qubits ao registrador, **aumentamos sua capacidade de armazenamento exponencialmente**, ou seja, **três qubits podem armazenar 8 números diferentes ao mesmo tempo**, **quatro qubits podem armazenar 16 números diferentes ao mesmo tempo**, e assim por diante; **em geral,  $L$  qubits podem armazenar  $2^L$  números ao mesmo tempo**. De forma simplificada, podemos dizer que **dois qubits** equivalem a 4 bits, **3 qubits** a 8 bits, **4 qubits** a 16 bits, e assim por diante. Se existissem  $n$  qubits, então esta tabela teria  $2n$  linhas.

Uma comparação do **número de qubits** de um computador quântico, com relação ao **número de bits** de um computador clássico, pode ser vista na Tabela 120.

Um **qubit** é mais do que isso. Ele pode, simultaneamente, representar os valores equivalentes a 0 e a 1. Pode estar numa **superposição de estados**, uma estranha propriedade quântica que potencializa a realização de cálculos em paralelo. Os **qubits** aumentam de maneira exponencial a capacidade de computação.

A **superposição de estados** é uma capacidade típica dos sistemas quânticos (sejam

1 qubit = 2 bits
2 qubits = 4 bits
3 qubits = 8 bits = 1 byte
4 qubits = 16 bits
5 qubits = 32 bits
6 qubits = 64 bits
7 qubits = 128 bits
8 qubits = 256 bits
9 qubits = 512 bits
10 qubits = 1.024 bits
13 qubits = 8.192 bits = 1 kilobytes
23 qubits = 8.388.608 bits = 1 megabyte
33 qubits = 8.589.934.592 bits = 1 gigabyte
43 qubits = 8.796.093.022.208 bits = 1 terabyte
44 qubits = 17.592.186.044.416 bits
45 qubits = 35.184.372.088.832 bits
n qubits = $2^n$ bits

Figura 120 – Tabela Qubits versus Bits: atualmente, já estamos em 79 qubits do computador quântico IonQ.

Fonte: <[https://pt.wikipedia.org/wiki/Bit\\_quântico](https://pt.wikipedia.org/wiki/Bit_quântico)>

eles formados por átomos, elétrons, fótons ou moléculas) de se comportar concomitantemente como partícula e onda. É a tal da **dualidade partícula-onda**. A situação se torna menos surreal quando se toma como exemplo a onda criada por uma pedra arremessada num lago. Ela causa oscilações na superfície da água na forma de círculos concêntricos que podem, ao mesmo tempo, atravessar duas pontes vizinhas na beira do lago. Nesse caso, se uma ponte for a representação do número 0 e outra do 1, parte da onda é 0 e parte é 1. A onda é 0 e 1 ao mesmo tempo. Mas um computador quântico que desse duas respostas para um problema seria de pouca valia. Afinal, apenas uma delas é a certa. Aí entra em ação um segundo fenômeno quântico, a interferência de ondas. Retomando ao exemplo do lago, depois de atravessar as duas pontes, a onda 1 e a onda 0 se reencontram. Essa interação pode ser destrutiva, as ondas se cancelam e o resultado final é 0. Ou construtiva, as ondas se somam e a resposta é 1.

Durante essa evolução, cada número na superposição é afetado e, como resultado, geramos uma computação paralela maciça, embora em uma peça de hardware quântico. Isso significa que um computador quântico pode em apenas um passo computacional executar a mesma operação matemática em números de entrada diferentes  $2^L$  codificados em superposições coerentes de  $L$  qubits. A fim de realizar a mesma tarefa, qualquer computador clássico deve repetir a mesma computação em  $2^L$  ou um deve usar dois processadores diferentes trabalhando em paralelo. Em outras palavras, um computador quântico oferece um enorme ganho no uso de recursos computacionais, como tempo e memória.

Os chamados algoritmos quânticos são instruções matemáticas, espécie de programas, que aumentam a probabilidade da *superposição de estados* e da *interação de ondas de levarem à resposta certa ao final do processamento de dados*. Estranho? Sim. Mas, bem-vindo ao mundo quântico. Uma vez que um registrador é preparado em



# A origem dos ganhos quânticos

Os efeitos da superposição de estados e da interferência de ondas

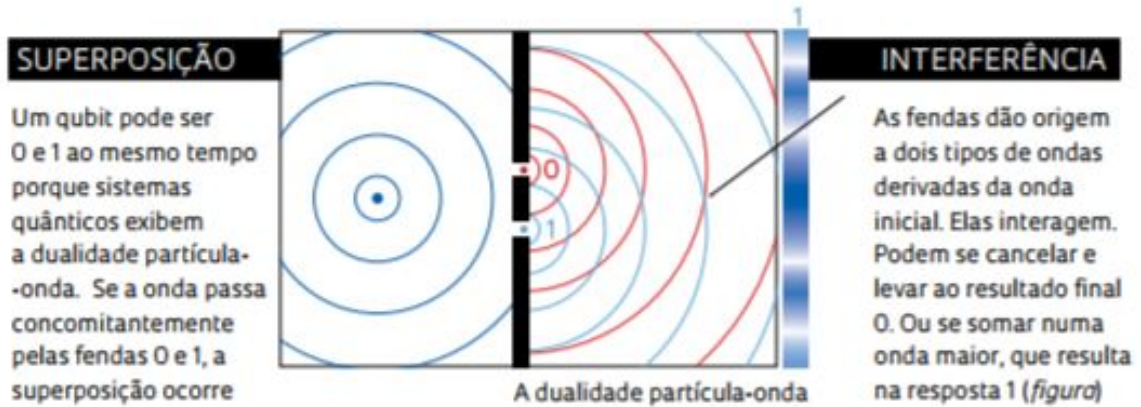


Figura 121 – Superposição, Interferência e a dualidade partícula-onda.

Fonte: <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>  
(PIVETTA, 2012)

uma superposição de números diferentes, podemos **executar operações** sobre todos esses números. Por exemplo, se qubits são átomos, os pulsos de laser adequadamente sintonizados afetam estados eletrônicos atômicos e desenvolvem superposições iniciais de números codificados em diferentes superposições.

Até 2007 parecia não haver outra resposta possível para a pergunta acima, a não ser atribuir as vantagens de uma máquina impulsionada por **qubits**, os bits quânticos, ao **emaranhamento** ou **entrelaçamento** quântico, misterioso e estranho fenômeno que aumentaria exponencialmente a capacidade de processamento de dados. Partículas, átomos ou moléculas descritos como *emaranhados* se encontram tão fortemente ligados entre si - os físicos usam o termo *correlacionados* - que são capazes de trocar informação independentemente de estarem lado a lado ou a milhares de quilômetros de distância. Apesar de poderoso, o **entrelaçamento** é também frágil, e apenas se mantém em situações especiais, em sistemas extremamente controlados, que não interagem com o ambiente externo (PIVETTA, 2012).

## 9.5.3 Implementando qubits

*Qubits* são compostos de partículas controladas (por exemplo, dispositivos que aprisionam partículas e as trocam de um estado para outro).

Em mecânica quântica, *nível de energia* é um estado quântico de uma partícula (como um elétron, um átomo ou uma molécula, por exemplo) cuja energia está bem definida ao longo do tempo. Um bit quântico ("qubit") pode ser imaginado considerando-se esses níveis de energia. Por exemplo, como o elétron nos dois níveis mais baixos de energia de um átomo de Hidrogênio.

Evidências de que os elétrons podem apresentar possíveis orientações em dois sentidos diferentes, (o *momento angular intrínseco* chamado *spin*) foram obtidas em 1921 pelos físicos alemães **Otto Stern** (1888-1969) e **Walther Gerlach** (1889-1979). Eles empregaram uma série de experiências, com a finalidade de comprovar as suas evidências.



Figura 122 – Otto Stern - um físico estadunidense nascido na Alemanha, laureado com o Nobel de Física de 1943.

Fonte: <[https://pt.wikipedia.org/wiki/Otto\\_Stern](https://pt.wikipedia.org/wiki/Otto_Stern)>

**Um computador quântico líquido** - Dois *qubits* são codificados manipulando o *spin* do núcleo de átomos de carbono e hidrogênio do clorofórmio. Ver a Figura 124 (PIVETTA, 2012).

Na mecânica quântica o termo **spin** (em inglês "giro") associa-se, sem rigor, às possíveis orientações que partículas subatômicas carregadas, como o próton e o elétron, e alguns núcleos atômicos podem apresentar quando imersas em um campo magnético. O termo *spin* em mecânica quântica liga-se ao vetor **momento angular intrínseco de uma partícula** e às diferentes orientações (quânticas) da partícula quando imersa em um campo magnético. Ver a Figura 125 e Figura 126 (PIVETTA, 2012).

O *spin* é uma propriedade que não se compara com nada que existe em nossa volta. Ele está associado com a maneira como os elétrons ocupam os níveis de energia no átomo. Um elétron pode ter o spin 'up' (para cima) ou 'down' (para baixo). Mas, essa nomenclatura é apenas para diferenciar duas situações, pois não existe 'para cima' e 'para baixo' nos átomos. O *spin* é uma característica intrínseca das partículas elementares.

Mas por que a propriedade do *spin* é tão importante?

**Propriedades magnéticas** - O *spin*, no caso dos elétrons, quando combinado com o *momento angular* que essas partículas possuem ao redor do átomo, é responsável pelas propriedades magnéticas da matéria. A interação entre o *spin* e o *momento*



Figura 123 – Walther Gerlach - um físico alemão, co-descobridor do experimento que descobriu os spins de Stern-Gerlach.

Fonte: <[https://pt.wikipedia.org/wiki/Walther\\_Gerlach](https://pt.wikipedia.org/wiki/Walther_Gerlach)>

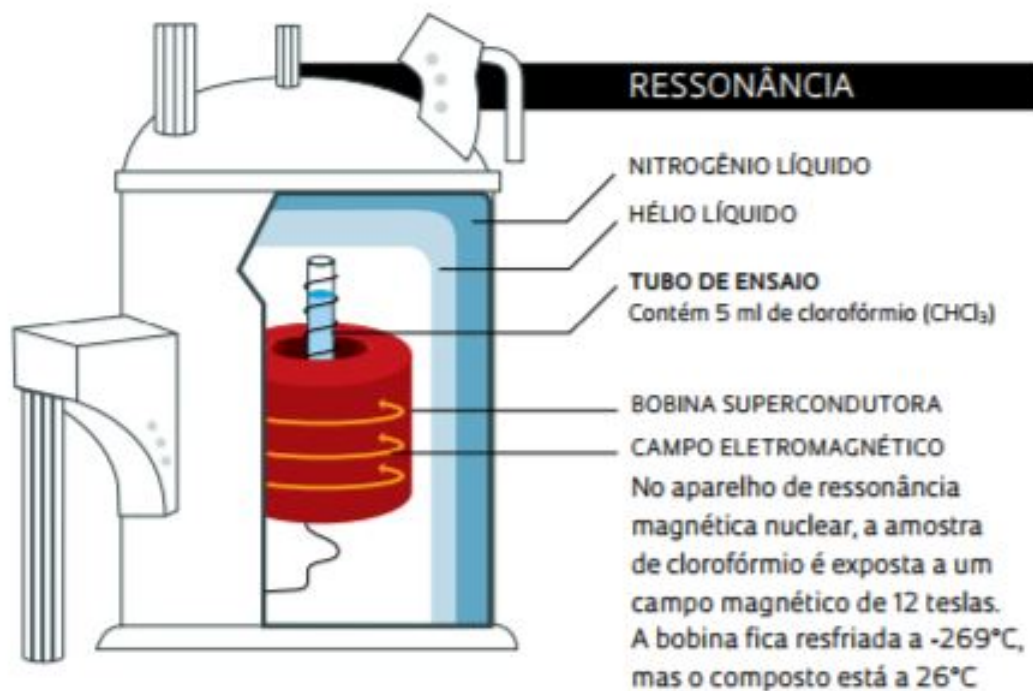


Figura 124 – Um computador quântico líquido.

Fonte: <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>

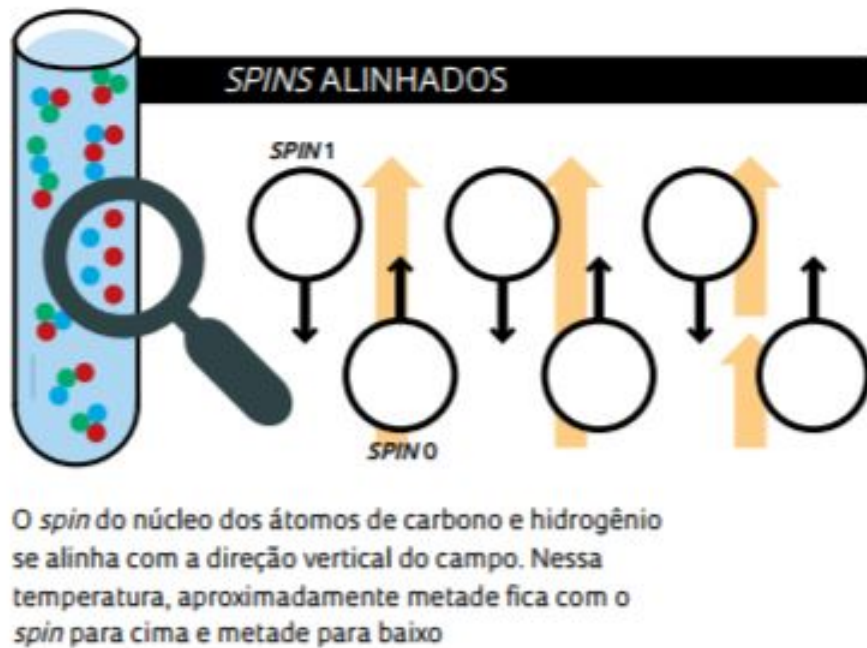


Figura 125 – Spins alinhados.

Fonte: <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>

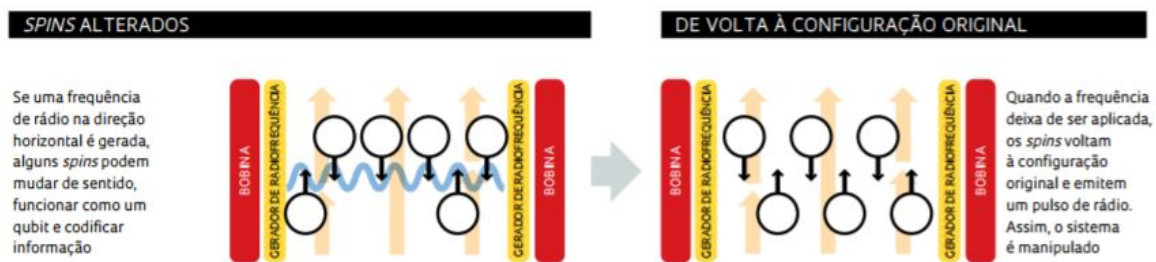


Figura 126 – Spins alterados e de volta à configuração original.

Fonte: <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>

*angular* é que faz com que surja o magnetismo da matéria. Materiais magnéticos têm uma infinidade de aplicações - dos ímãs de geladeira para fixarmos os recados que não queremos esquecer aos ímãs utilizados em motores elétricos, passando pelos materiais utilizados para a gravação magnética de informação nos discos rígidos dos computadores.

A maior parte das informações existentes atualmente está gravada magneticamente em discos rígidos nos computadores espalhados por todo mundo. A gravação de cada informação é feita por meio da aplicação de campos magnéticos sobre o material magnético do sistema de gravação. As informações são gravadas na forma de um código binário, como uma sequência de '0' e '1'. Pode-se representar, por exemplo, o '0' como o polo norte de um pequeno ímã apontando para cima e o '1' com o polo norte apontando para baixo.

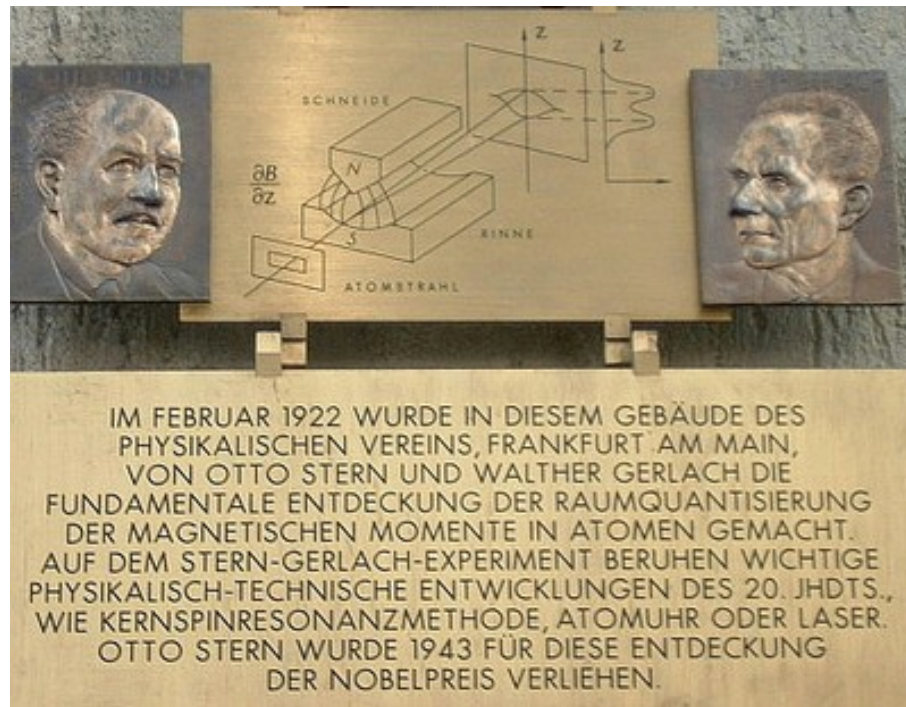


Figura 127 – A placa acima, no Instituto de Física de Frankfurt (Alemanha), comemora o experimento de Stern (à esquerda) e Gerlach que levou à descoberta do 'spin' (foto: Wikimedia Commons/Peng - CC 3.0 BY-SA).

Fonte: <[http://www.cienciahoje.org.br/noticia/v/ler/id/2781/n/o\\_spin\\_que\\_move\\_o\\_mundo](http://www.cienciahoje.org.br/noticia/v/ler/id/2781/n/o_spin_que_move_o_mundo)>

**Processamento de informação** - O *spin* dos elétrons também pode ser utilizado para uma nova aplicação que no momento está em desenvolvimento, para não somente armazenar informações, mas também processá-las. Os computadores atuais processam informações utilizando circuitos eletrônicos baseados no controle do fluxo de corrente elétrica através dos seus componentes. O processador de um computador realiza centenas de milhões de operações por segundo por meio do controle do fluxo de corrente elétrica através dos milhões de componentes em seu interior. Contudo, há um novo modelo que poderá substituir essa forma de processar informações. Ela se chama **spintrônica** - a eletrônica de *spins*, que tem como objetivo controlar o fluxo de corrente em um dispositivo, não somente pela carga dos elétrons, mas também pelo *spin*. A carga elétrica do elétron é afetada pela ação de *campos elétricos*, mas o *spin* é afetado por *campos magnéticos*. Essa nova proposta poderá produzir dispositivos mais rápidos e que dissipem menos energia.

Além disso, a utilização do *spin* no processamento de informações permitirá o desenvolvimento de novos algoritmos de computação, que poderão utilizar as propriedades quânticas do *spin*. Esse novo ramo de conhecimento chama-se de *computação quântica*. A descoberta de uma propriedade inusitada como o *spin* levou a uma melhor compreensão dos fenômenos magnéticos e estes permitiram o desenvolvimento de novas formas de processar e armazenar informações. Talvez em um futuro próximo possamos utilizar essa propriedade de forma que sequer somos capazes de imaginar, pois com certeza ainda não esgotamos todas as possibilidades que a Física Quântica nos apresenta.

### 9.5.4 Caracterizando o Computador Universal Quântico

O computador quântico é primeiramente uma máquina que é uma construção teórica, cujo propósito é permitir o processamento de informação quântica ser analisado formalmente. Em particular, ele estabelece o *Princípio de Church-Turing* introduzido na seção 9.1. Eis uma "receita" para um computador quântico, baseada naquela de **Deutsch**: Um computador quântico é um conjunto de  $n$  qubits sobre os quais as seguintes operações são experimentalmente possíveis:

- Cada **qubit** pode ser preparado em algum estado, por exemplo,  $|0\rangle$  ou  $|1\rangle$ .
- Cada **qubit** pode ser medido na base  $\{|0\rangle, |1\rangle\}$ .
- Uma **porta quântica universal** (ou conjunto de portas) pode ser aplicada para qualquer subconjunto de tamanho fixo dos **qubits**.
- Os **qubits** não evoluem, a não ser via as transformações supracitadas.

Estes itens circundam as ideias principais. O modelo físico de computação para se projetar tal computador é o modelo em malha (*network model*), em que portas lógicas quânticas (ver seção 3.4) são aplicadas sequencialmente em um conjunto de qubits. Em um computador clássico eletrônico, portas lógicas estão espalhadas espacialmente em uma placa de circuitos, mas no computador quântico, tipicamente imaginam-se as portas lógicas como interações ligadas e desligadas no tempo (como já foi explicado), com os qubits em posições fixas.

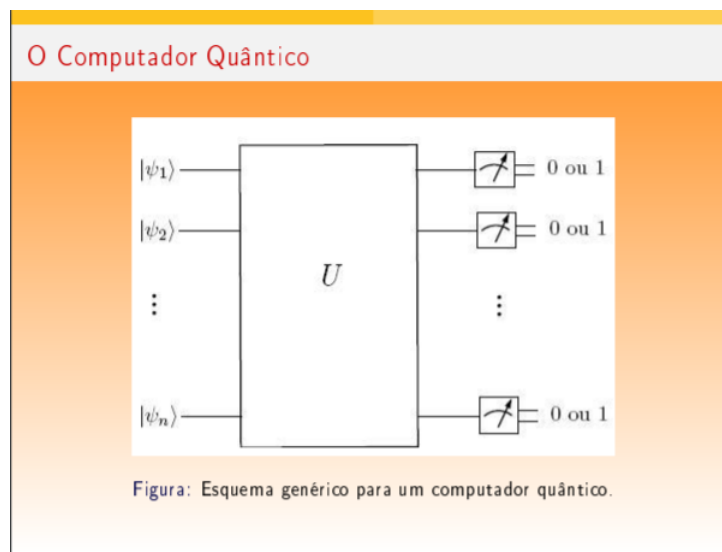


Figura 128 – O esquema genérico para um computador quântico de  $n$  qubits.

Fonte: <[www.lncc.br/pdf\\_consultar.php?idt\\_arquivo=2445&mostrar=1](http://www.lncc.br/pdf_consultar.php?idt_arquivo=2445&mostrar=1)>

## 9.6 Bibliografia e Fonte de Consulta

Ronan, Colin A. (1987). História Ilustrada da Ciência. Universidade de Cambridge. III - Da Renascença à Revolução Científica 1 ed. São Paulo: Círculo do Livro.

Henry, John, (1998). *A Revolução Científica e as Origens da Ciência Moderna* 1 ed. [S.l.: s.n.] ISBN 9788571104426

Bernhard Ömer, *Structured Quantum Programming*, first version, 26th May 2003, last revision, 2nd September 2009, Institute for Theoretical Physics, Vienna University of Technology. <<http://tph.tuwien.ac.at/~oemer/doc/structqprog.pdf>>

A Onda dos Qubits - o conceito de Discórdia Quântica - <<http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>>

O Spin que move o mundo - <[http://www.cienciahoje.org.br/noticia/v/ler/id/2781/n/o\\_spin\\_que\\_move\\_o\\_mundo](http://www.cienciahoje.org.br/noticia/v/ler/id/2781/n/o_spin_que_move_o_mundo)>

Limite Quântico x Limite Clássico - <<https://otelhado.wordpress.com/2010/08/16/o-que-define-algo-como-...>>

Classical limit of quantum mechanics - <[www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1806-11172003000200006](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1806-11172003000200006)>

Limite Clássico da mecânica quântica - Revista Brasileira de Ensino - <[www.ebah.com.br/content/ABAAAUTEAE/limite-classico-mecanica-quantica](http://www.ebah.com.br/content/ABAAAUTEAE/limite-classico-mecanica-quantica)>

Constante de Planck - <[http://www.ifsc.usp.br/~lavfis/images/.../CtePlanck\\_1.pdf](http://www.ifsc.usp.br/~lavfis/images/.../CtePlanck_1.pdf)>

Computação Quântica - <[https://pt.wikipedia.org/wiki/Computacao\\_quantica](https://pt.wikipedia.org/wiki/Computacao_quantica)>

Constante de Planck: Uma Nova Visão para o Ensino Médio - <[http://qnesc.sbq.org.br/online/qnesc33\\_4/246-EEQ-6011.pdf](http://qnesc.sbq.org.br/online/qnesc33_4/246-EEQ-6011.pdf)>

História da Mecânica Quântica - <[https://pt.wikipedia.org/wiki/Historia\\_da\\_mecanica\\_quantica](https://pt.wikipedia.org/wiki/Historia_da_mecanica_quantica)>

Max Planck: the reluctant revolutionary - <<http://physicsworld.com/cws/article/print/2000/dec/01/max-planck-the-reluctant-revolutionary>>

Teoria de Max Planck - <<http://brasilecola.uol.com.br/quimica/teoria-max-planck.htm>>

EISBERG, Robert e RESNICK, Robert. *Física Quântica - Átomos, Moléculas, Sólidos, Núcleos e Partículas*. Tradução de Paulo Costa Ribeiro, Ênio Costa da Silveira e Marta Feijó Barroso. Rio de Janeiro: Campus, 1979.

## 9.7 Para saber mais

A. Hermann: *Lexikon - Geschichte der Physik A-Z* (1978). Aulis-Verlag Deubner & Co KG.

J. Branson: *Quantum Physics 130A* (2001). lecture notes, <[http://heppc16.ucsd.edu/ph130a/130a\\_notes/node15.html](http://heppc16.ucsd.edu/ph130a/130a_notes/node15.html)>.

D.C. Cassidy: *Exhibit on Werner Heisenberg* (1998). American Institute of Physics, <[http://www.aip.org/history/heisenberg/p09\\_text.htm](http://www.aip.org/history/heisenberg/p09_text.htm)>.

A. Einstein, B. Podolsky, N. Rosen: *Can quantum-mechanical description of physical reality be considered complete?* (1935). *Physical Review* 47, pp. 777-780.

R. Solovay and V. Strassen: *A Fast Monte-Carlo Test for Primality* (1977). *SIAM Journal on Computing*, 1977, pp. 84-85.

M.A. Nielsen and I.L. Chuang: *Quantum Computation and Quantum Information* (2000). Cambridge University Press.

M. Agrawal, N. Kayal, N. Saxena: *PRIMES is in P* (2002). preprint, <<http://www.cse.iitk.ac.in/users/manindra/primality.ps>>.

D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer* (1985). *Proc. R. Soc., London, A* 400, pp.97-117.

K. Svozil: *Quantum algorithmic information theory* (1996). *Journal of Universal Computer Science* 2, pp. 311-346

D. Deutsch and R. Jozsa: *Rapid solution of problems by quantum computer* (1992). *Proc. Roy. Soc. London, Ser. A*, vol. 439, pp.553-558.

R.P. Feynman: *Quantum mechanical computers* (1985). *Optics News* 11, pp 11-20.

P. W. Shor: *Algorithms for quantum computation: Discrete logarithms and factoring* (1994). *Proceeding. 35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, CA.

Lov K. Grover: *A fast quantum mechanical algorithm for database search* (1996). *Proceeding of the 28th Annual ACM Symposium on Theory of Computing*.

J.I. Cirac, P. Zoller: *Quantum Computations with Cold trapped Ions* (1995). *Phys. Rev. Lett.* 74, p. 4091.

I.L. Chuang et al.: *NMR quantum computing: Realizing Shor's algorithm* (2001). *Nature* 414, pp. 883-887.

Quantum Computation and Quantum Information. [S.l.]: por Nielsen, M. e I. Chuang (2000) Cambridge University Press, 2000. |ISBN= 0-521-63503-9.

Mosca, M. (2008). Quantum Algorithms. arXiv:0808.0369Acessível livremente [quant-ph].

Shor's Algorithm por Roger Herrigel e Wojciech De Roeck em 14 de abril de 2008.

Photons set fresh quantum computing record por Jacob Aron em 23 de outubro de 2012.





## Uma Introdução à Computação Quântica

O Húngaro de origem judaica **John von Neumann** (1903-1957), nascido *Margittai Neumann János Lajos*, foi um matemático naturalizado estadunidense. John von Neumann cresceu de criança prodígio para um dos matemáticos mais proeminentes do mundo aos seus vinte e cinco anos. Um trabalho importante na Teoria dos Conjuntos de Georg Cantor, inaugurou uma carreira que tocou quase em todos os principais ramos da Matemática. O dom de **Von Neumann** para a matemática aplicada levou seu trabalho a direções que influenciaram, também, a *Teoria Quântica*, iniciada a partir **Max Planck** (1858-1947), um físico alemão, considerado o precursor da Física Quântica e um dos físicos mais importantes do século XX, laureado com o Nobel de Física de 1918, por suas contribuições na área.



Figura 129 – John von Neumann - A modelagem algébrica da teoria quântica com os espaços de Hilbert.

Fonte: Google Images <[dailynewshungary.com](http://dailynewshungary.com)>

## 10.1 A contribuição de John von Neumann à Teoria Quântica

**Carreira Europeia (1921-1930) - David Hilbert** foi um matemático alemão. Foi eleito membro estrangeiro da Royal Society em 1928. **David Hilbert** é um dos mais notáveis matemáticos, e os tópicos de suas pesquisas são fundamentais em diversos ramos da matemática atual. **John von Neumann** iniciou sua carreira intelectual numa época em que a influência de **David Hilbert** (1862-1943) e seu programa de estabelecimento de fundamentos axiomáticos para a Matemática estava no auge. Um artigo escrito enquanto ainda estava no *Lutheran Gymnasium* ("*Introduction of Transfinite Ordinals*", de 1923), forneceu a definição agora convencional de um número ordinal como o conjunto de todos os números ordinais menores. Isso evita algumas das complicações levantadas pelos números transfinitos de **Georg Cantor**. "*Axiomatization of Set Theory*" de **Von Neumann** (1925) despertou a atenção do próprio **Hilbert**. De 1926 a 1927, **Von Neumann** fez um trabalho de pós-doutorado sob a orientação de **Hilbert** na Universidade de Göttingen. O objetivo de axiomatizar a matemática foi derrotado pelos teoremas de incompletude de **Kurt Gödel**, uma barreira que foi entendida imediatamente por **Hilbert** e **John von Neumann**.

Em meados dos anos 20 - **John von Neumann** se viu apontado como um prodígio em conferências. **Von Neumann** produziu uma sucessão impressionante de artigos fundamentais em Lógica, Teoria dos Conjuntos, Teoria dos Grupos, Teoria Ergódica e Teoria dos Operadores. Em 1929, **John von Neumann** foi convidado a dar uma palestra sobre *Teoria Quântica* na *University of Princeton*. Isso o levou a uma nomeação como professor visitante nos anos de 1930 a 1933 e tornou-se um dos primeiros professores do *Advanced Studies Institute* em *Princeton*, New Jersey, USA. Motivado por um desejo contínuo de desenvolver técnicas matemáticas adequadas aos fenômenos quânticos, *Von Neumann*, de 1929 até a década de 1940, introduziu uma *Teoria de Anéis de Operadores*, agora conhecida como álgebras de **Von Neumann**.

**Princeton (1930-1942) - Computação Quântica** - A velocidade de processamento exponencialmente maior do que o mais avançado computador atual, deu origem à Computação Quântica. Isso é uma das vantagens que se espera do sistema computacional baseado nos conceitos da Física Quântica: o computador quântico. A Computação Quântica é fundamentada em conceitos criados pela Física Quântica como o da *sobreposição/superposição* (quando uma partícula está em diferentes condições contraditórias simultaneamente) e do *entrelaçamento/emaranhamento* (quando a alteração em uma partícula provoca o mesmo efeito em outra que se encontra distante). Não se sabe se os eventos da mecânica quântica seriam todos *Turing-computáveis*, mas se sabe que modelos rigorosos, como as *Máquinas de Turing Quânticas* (MTQ), já foram construídos. Em 1932, **John von Neumann** publicou o seu livro sobre os fundamentos matemáticos da mecânica quântica, que pode ser visto na Figura 130.

## 10.2 Máquina de computação e o princípio de Church-Turing

Na introdução do artigo ([DEUTSCH, 1985](#)), **Deutsch** escreveu:

A teoria das máquinas de computação foi extensamente desenvolvida durante as últimas décadas. Intuitivamente, uma máquina de computação é qualquer sistema físico cuja evolução dinâmica leva de um conjunto de estados "de entrada" para um de um conjunto de estados de "saída". Os estados são rotulados em alguma maneira

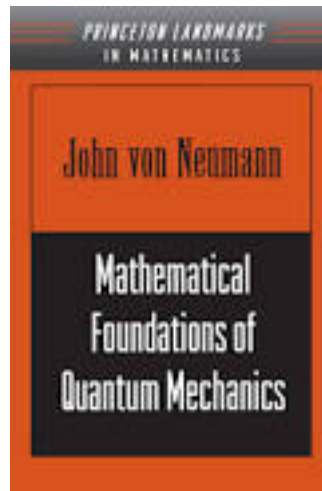


Figura 130 – John von Neumann - The Mathematical Foundations of Quantum Mechanics.

Fonte: <<https://universosquanticos.wordpress.com/2017/04/26/pioneiros-quanticos-paul-benioff/>>

canônica maneira, a máquina é preparada em um estado com um determinado rótulo de entrada e, em seguida, após alguma evolução, o estado de saída é medido. Para um sistema determinístico clássico, o rótulo de saída medido é uma função  $f$  do rótulo de entrada; além disso, o valor desse rótulo pode, em princípio, ser medido por um observador externo (o "usuário") e a máquina é chamada para "computar" a função  $f$ .

Duas máquinas computacionais determinísticas clássicas são "computacionalmente equivalentes" sob determinadas rotulações de seus estados de entrada e saída, se computarem a mesma função sob essas rotulações. Mas, máquinas de computação quântica e, na verdade, máquinas de computação estocásticas clássicas, não 'computam funções' no sentido acima: o estado de saída de uma máquina estocástica é aleatório, onde somente a função de distribuição de probabilidade, para as possíveis saídas, dependem do estado de entrada. O estado de saída de uma máquina quântica, embora totalmente determinada pelo estado de entrada não é um observável e assim o usuário não pode, em geral, descobrir seu rótulo. No entanto, a noção de equivalência computacional pode ser generalizada para aplicar a essas máquinas também.

Novamente, definimos a equivalência computacional sob certas rotulações, mas agora é necessário especificar, mais precisamente, o que deve ser rotulado. No que diz respeito à entrada, os rótulos devem ser dados para cada um dos possíveis modos de preparar a máquina, que correspondem, por definição, a todos os possíveis estados de entrada. Isso é idêntico ao caso determinístico clássico. No entanto, há uma assimetria entre a entrada e a saída porque existe uma assimetria entre a preparação e a medição: enquanto que um sistema quântico pode ser preparado em qualquer estado de entrada permitido, a medição não pode, em geral, determinar seu estado de saída; em vez disso, deve-se medir o valor de alguns *observáveis*. Ao longo do artigo (DEUTSCH, 1985), Deutsch utilizou a equação de **Schrödinger**, na qual o estado quântico é uma função do tempo, sendo os observáveis, *operadores* algébricos. Assim, o que deve ser rotulado é o conjunto de pares ordenados, consistindo de uma *saída observável* e um possível *valor medido* daquele observável (na teoria quântica,

um *operador Hermitiano* e um de seus *autovalores*). Esse par ordenado contém, com efeito, a especificação de um possível experimento que poderia ser feito na saída, juntamente com um possível resultado dessa experiência.

Duas máquinas de computação são computacionalmente equivalentes sob determinadas rotulações se, em qualquer experimento ou sequência de experimentos possíveis, as suas entradas foram preparadas de forma equivalente sob as rotulações de entrada e os observáveis correspondentes sob as rotulações de saída medidos, os valores medidos desses observáveis para as duas máquinas são estatisticamente indistinguíveis. Isto é, as funções de distribuição de probabilidade para as saídas das duas máquinas devem ser idênticas.

No sentido que acabamos de descrever, uma dada máquina computacional  $\mathcal{M}$  computa no máximo uma função. No entanto, não deve haver diferença fundamental entre alterar o estado de entrada em que  $\mathcal{M}$  é preparada, e alterando sistematicamente a constituição de  $\mathcal{M}$  para que se torne uma máquina diferente  $\mathcal{M}'$  computando uma função diferente. Para formalizar tais operações, muitas vezes é útil considerar máquinas com duas entradas, a preparação de uma constituindo um "programa" determinando qual função da outra é para ser computada. Para cada uma dessas máquinas  $\mathcal{M}$ , corresponde um conjunto  $C(\mathcal{M})$  de ' $\mathcal{M}$ -funções computáveis'. Uma função  $f$  é  $\mathcal{M}$ -computável, se  $\mathcal{M}$  puder calcular  $f$  quando preparada com algum programa. O conjunto  $C(\mathcal{M})$  pode ser ampliado, estendendo-se o conjunto de mudanças na constituição de  $C(\mathcal{M})$  que estão rotulados como possíveis programas- $\mathcal{M}$ . Dadas duas máquinas  $\mathcal{M}$  e  $\mathcal{M}'$ , é possível construir uma máquina composta, cujo conjunto de funções computáveis, corresponde à união de  $C(\mathcal{M})$  e  $C(\mathcal{M}')$ .

Não há razão puramente lógica para que alguém não pudesse continuar *ad infinitum* construindo mais poderosamente máquinas de computação, nem porque deve existir qualquer função que esteja fora do conjunto computável de cada máquina fisicamente possível. No entanto, embora a lógica não proíba o cálculo físico de funções arbitrárias, parece que a Física o faz. Como é bem conhecido, ao projetar máquinas de computação, uma máquina atinge rapidamente um ponto quando a adição de hardware adicional não altera o conjunto de funções computáveis da máquina (sob a idealização de que a capacidade de memória é, na verdade, ilimitada); além disso, para funções dos inteiros  $\mathbb{Z}$  para  $\mathbb{Z}$ , o conjunto  $C(\mathcal{M})$  está sempre contido em  $C(\mathcal{T})$ , onde  $\mathcal{T}$  é a máquina de computação universal de **Turing** (**TURING, 1936**) (*On the Computable Numbers with an application to the Entscheidungsproblem*).  $C(\mathcal{T})$  em si, também conhecido como o conjunto de funções recursivas, é *enumerável* e, portanto, infinitamente menor que o conjunto de todas as funções de  $\mathbb{Z}$  a  $\mathbb{Z}$ .

(**CHURCH, 1936**) e (**TURING, 1936**) conjecturaram que essas limitações sobre o que pode ser computado, não são impostas pelo estado-da-arte na concepção de máquinas de computação, nem pela nossa ingenuidade em construir modelos para computação, mas são universais. Isso é chamado de "**Hipótese de Church-Turing**"; de acordo com **Turing**:

*Every 'function which would naturally be regarded as computable' can be computed by the universal Turing machine. (1)*

"Toda função naturalmente considerada como computável, pode ser computada pela máquina universal de Turing."

A visão convencional e não-física desta hipótese, interpreta-a como uma conjectura quase matemática, que todas as formalizações possíveis da noção matemática intuitiva de "algoritmo" ou "computação" são equivalentes entre si. Mas, **Deutsch** mostra em (DEUTSCH, 1985), que também pode ser considerado como afirmando um novo princípio físico, que Deutsch chamou de "**Princípio de Church-Turing**", para distingui-lo de outras implicações e conotações da conjectura (1). A "**Hipótese Church-Turing**" (1) e outras formulações existentes na literatura (ver Hofstadter (1979) para uma interessante discussão de várias versões) são muito vagas em comparação com princípios físicos tais como as leis da termodinâmica ou o princípio da equivalência gravitacional. Mas será visto abaixo, que a declaração de **Deutsch**, do "**Princípio da Church-Turing**" (2) é manifestamente física e inequívoca. **Deutsch** (DEUTSCH, 1985) mostrou que tem o mesmo status epistemológico de outros princípios físicos.

Deutsch propôs reinterpretar as '*funções de Turing que naturalmente seriam consideradas computáveis*' como as funções que podem, em princípio, ser computadas por um sistema físico real. Pois, certamente, seria difícil considerar uma função 'natural' como computável, se não pudesse ser computada *in Nature*, e contrariamente. Para este fim, Deutsch definiu a noção de '*simulação perfeita*'. Uma máquina de computação  $\mathcal{M}$  é capaz de simular perfeitamente um sistema físico  $\mathcal{S}$ , sob uma dada rotulação de suas entradas e saídas, se existir um programa ( $\mathcal{S}$ ) para  $\mathcal{M}$ , que torne  $\mathcal{M}$  computacionalmente equivalente a  $\mathcal{S}$  nessa rotulação. Em outras palavras, ( $\mathcal{S}$ ) converte ( $\mathcal{M}$ ) em uma 'caixa preta' funcionalmente indistinguível de ( $\mathcal{S}$ ). Com isso, **Deutsch** pôde declarar a versão física do "**Princípio de Church-Turing**":

*"Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means."* (2)

"Cada sistema físico finitamente realizável pode ser perfeitamente simulado por uma máquina de computação de modelo universal operando por meios finitos."

Esta formulação é melhor definida e mais física do que a própria maneira de **Turing** (1), porque se refere exclusivamente a conceitos objetivos, como "medição", "preparação" e "sistema físico", que já estão presentes na **teoria da medida**. Isso evita a terminologia como "naturalmente ser considerado", o que não se encaixa bem na estrutura existente da Física. Os sistemas físicos "finitamente realizáveis" referidos em (2) devem incluir qualquer objeto físico em que a experimentação é possível. A "máquina universal de computação", por outro lado, precisa ser apenas um modelo idealizado (mas, teoricamente permitido) finamente especificável. As rotulações implicitamente referidas em (2) deve também ser finitamente especificável. A referência em (1) a uma máquina de computação universal específica (**Turing's**) tem sido necessariamente substituída por (2), pelo requisito mais geral de que esta máquina funcione "por meios finitos". ('Finite means') podem ser definidos axiomaticamente, sem hipóteses sobre a forma de leis físicas (GANDY, 1953) (GANDY, 1980) <sup>1</sup>

Se pensarmos em uma máquina de computação como procedendo em uma sequência de etapas cuja duração tem um limite inferior diferente de zero, então ele opera por

<sup>1</sup> **Robin Oliver Gandy** (1919-1995) foi um matemático e lógico britânico. Era amigo, estudante e sócio de **Alan Turing**, tendo sido supervisionado por **Turing** durante seu PhD na University of Cambridge, onde eles trabalharam juntos.

"meios finitos" se (i) apenas um subsistema finito (embora, nem sempre o mesmo) está em evolução durante qualquer passo, e (ii) a evolução só depende sobre o estado de um subsistema finito, e (iii) a regra que especifica a evolução pode ser dada finitamente no sentido matemático (por exemplo, como um inteiro). Máquinas de Turing satisfazem essas condições, e assim, o computador quântico universal  $\mathcal{Q}$ .

A afirmação do princípio da Church-Turing (2) é mais forte do que o estritamente necessário por (1). De fato, é tão forte que não é satisfeito pela máquina de **Turing** na física clássica. Em (DEUTSCH, 1985), na sua introdução, a conclusão é que, **a teoria quântica é compatível com a forma forte (2) da afirmativa empírica do Princípio de Church-Turing**. O critério usual para o status empírico de uma teoria é que ela seja experimentalmente falsificável (POPPER, 1959) ("*One of the most important philosophical works of our century*".), ou seja, que exista observações em potencial que a contradiz.

**Karl Raimund Popper** (1902-1994) (Figura 131) foi um filósofo e professor austro-britânico. Amplamente considerado um dos maiores filósofos da ciência do século 20, **Popper** é conhecido por sua rejeição das visões indutivistas clássicas sobre o método científico em favor do falsificacionismo.

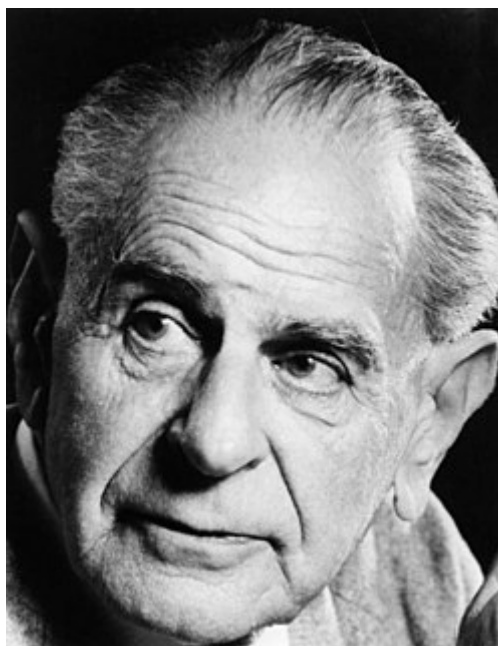


Figura 131 – Karl Popper - considerado um dos maiores filósofos da ciência do século 20, pensador sobre a lógica da pesquisa científica.

Fonte: <[https://pt.wikipedia.org/wiki/Karl\\_Popper](https://pt.wikipedia.org/wiki/Karl_Popper)> Veja sobre Karl Popper no vídeo <[https://www.youtube.com/watch?v=iamEsN\\_Ap9Q](https://www.youtube.com/watch?v=iamEsN_Ap9Q)>

### 10.3 Os pioneiros do computador quântico

Para aplicações com necessidade de capacidade de processamento exponencialmente maior do que os processadores clássicos oferecem hoje, foram introduzidas as primeiras ideias sobre o computador quântico, no início da década de 80, por

**Paul Benioff** (1930-). Em 1981, um físico americano que ajudou a criar o campo da computação quântica no *Argonne National Laboratory*, **Paul Benioff**, foi o primeiro a aplicar os princípios da física quântica à computação, teorizando sobre a criação de uma *máquina de Turing quântica*.

**Benioff** (1982) construiu um modelo para computação dentro da cinemática e dinâmica quântica, mas ainda é efetivamente clássico no sentido da seção anterior. É construído de modo que, no final de cada etapa computacional elementar, nenhuma propriedade caracteristicamente quântica do modelo - interferência, não-separabilidade, ou indeterminismo - pode ser detectado. Seus cálculos podem ser perfeitamente simulados por uma máquina de **Turing** (DEUTSCH, 1985). **Paul A. Benioff** é um físico **Benioff** é mais conhecido por sua pesquisa em teoria da informação quântica que demonstrou a possibilidade teórica de computadores quânticos. Em 2000, **Benioff** recebeu o *Quantum Communication Award of the International Organization for Quantum Communication, Computing, and Measurement*, bem como o *Quantum Computing and Communication Prize* da Universidade de Tama-gawa, no Japão. Tornou-se membro  *fellow* da Sociedade Americana de Física em 2001. No ano seguinte, foi agraciado com the *Special University of Chicago Medal for Distinguished Performance at Argonne National Laboratory*. Em 2016, *Argonne* realizou uma conferência em homenagem ao seu trabalho de computação quântica.



Figura 132 – Paul Benioff - Pioneiro na pesquisa em teoria da informação quântica que demonstrou a possibilidade teórica de computadores quânticos.

Fonte: <<https://universosquanticos.wordpress.com/2017/04/26/pioneiros-quanticos-paul-benioff/>>

**Benioff** deixou muitos artigos escritos sobre diversos aspectos da computação quântica, e muitos podem ser lidos nos links que seguem:

- Artigos de **Benioff** no site da *Argonne National Lab* (<[https://www.phy.anl.gov/theory/staff/Benioff\\_P.html](https://www.phy.anl.gov/theory/staff/Benioff_P.html)>)
- Artigos de **Benioff** no site Arxiv (<[https://arxiv.org/a/benioff\\_p\\_1.html](https://arxiv.org/a/benioff_p_1.html)>)

Em 2016 um simpósio em homenagem as suas contribuições foi realizado em *Argonne*, com o nome "*Quantum Computing: Beginnings to Current Frontiers*". As mais importantes contribuições de **Benioff** para a computação quântica foram 3 artigos escritos no início da década de 80, foram eles:

*The computer as a physical system: A microscopic quantum mechanical Hamiltonian*



*model of computers as represented by Turing machines* - Neste artigo, **Benioff** desenvolveu o primeiro modelo quântico com *mecânica hamiltoniana* para uma *máquina de Turing*. Ver em: <<https://link.springer.com/article/10.1007%2F0111339>>.

*Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: Application to Turing machines.* - Neste artigo, **Benioff** estendeu o seu trabalho anterior. Ver em: <<https://link.springer.com/article/10.1007%2F01857725>>

*Quantum mechanical hamiltonian models of turing machines* - Neste artigo, **Benioff** também estendeu o seu trabalho anterior. Ver em: <<https://link.springer.com/article/10.1007%2F01342185>>

Estes 3 artigos da década de 80 formaram a fundação teórica em que se desenvolveu a computação quântica.

A primeira ideia de um aparato computacional (máquina de **Turing**) utilizando propriedades quânticas foi idealizada por **Paul Benioff**. **Benioff** (1982) construiu um modelo para computação dentro da cinemática e dinâmica quântica, mas ainda é efetivamente clássico no sentido acima. É construído de modo que, no final de cada etapa computacional elementar, nenhuma propriedade caracteristicamente quântica do modelo - interferência, não-separabilidade, ou indeterminismo - pode ser detectado. Seus cálculos podem ser perfeitamente simulados por uma máquina de Turing. (**DEUTSCH**, 1985)

Foi **Benioff** quem primeiro reconheceu a importância de um artigo de 1973 do **Charles Bennett** (**BENNETT**, 1973), físico da IBM, onde era mostrada a possibilidade teórica da realização de *operações computacionais reversíveis*. O autômato de computação de propósito geral usual (por exemplo, uma máquina de **Turing**) é logicamente irreversível - sua função de transição não possui um inverso de valor único. O trabalho de **Bennett** mostrou que tais máquinas podem ser logicamente reversíveis a cada passo, enquanto retêm sua simplicidade e sua capacidade de fazer cálculos gerais. Este resultado é de grande interesse físico porque torna plausível a existência de computadores termodinamicamente reversíveis que poderiam realizar cálculos úteis a uma velocidade útil, enquanto dissipam consideravelmente menos energia por passo lógico. No primeiro estágio de sua computação, o autômato logicamente reversível é paralelo ao correspondente autômato irreversível, exceto pelo fato de salvar todos os resultados intermediários, evitando assim a operação irreversível do apagamento. O segundo estágio consiste em imprimir a saída desejada. O terceiro estágio então, reversivelmente, descarta todos os resultados intermediários indesejados (**BENNETT**, 1973).

No entanto, a proposta da máquina de **Benioff** não era exatamente um computador quântico, como explicado no segundo parágrafo desta seção.

Dois anos depois, a possibilidade de que efeitos quânticos poderiam oferecer algo verdadeiramente novo foi apontada pela primeira vez por **Richard Feynman** (**FEYNMAN**, 1982b). Em 1982, **Richard Feynman** considerou que efeitos quânticos poderiam oferecer algo realmente novo. Ele mostrou como um sistema quântico poderia ser usado para fazer cálculos. Além de explicar como tal máquina seria capaz de agir como um simulador para a física quântica. Um físico poderia realizar experiências de

física quântica usando um computador baseado na mecânica quântica. **Feynman** também argumentou que nenhuma máquina de **Turing** (clássica) seria capaz de simular alguns fenômenos quânticos sem introduzir um *fator exponencial* em seu desempenho. Assim, ele propôs que apenas um "*simulador quântico universal*" seria capaz de simular um sistema quântico eficientemente. **Surgia então a ideia de um computador quântico.**

**Richard Philips Feynman** (1918-1988) foi um físico norte-americano do século XX, um dos pioneiros da eletrodinâmica quântica, que também contribuiu com as primeiras ideias do computador quântico. **Feynman** trabalhou como professor no *California Institute of Technology* (1950-1988), foi um dos ganhadores do Prêmio Nobel de Física (1965) por pesquisas em eletrodinâmica quântica, juntamente com outro americano da *Harvard University, Cambridge, MA*, **Julian Schwinger**, e o japonês **Shin'Ichiro Tomonaga** da *Tokio Education University*.

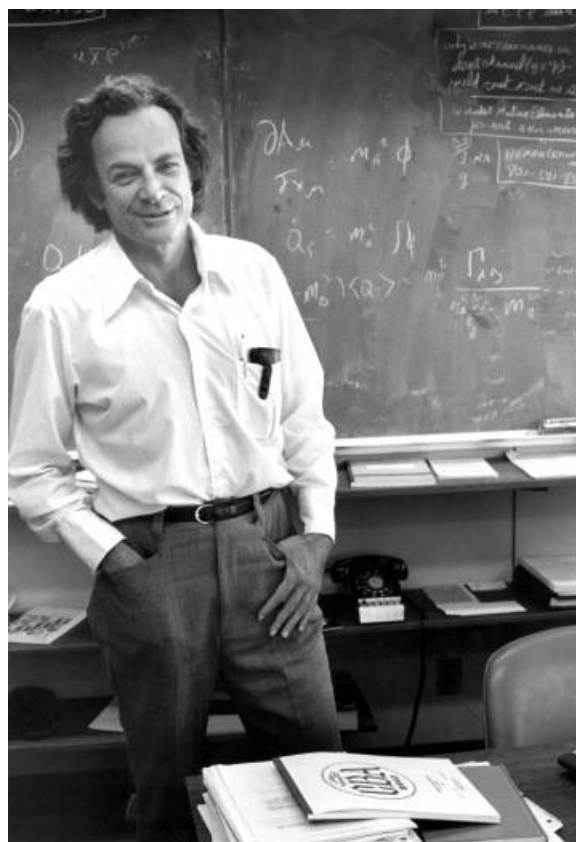


Figura 133 – Richard Feynman - O pioneiro na eletrodinâmica quântica e na área de computação quântica, introduzindo o conceito de nanotecnologia.

Fonte: Google Images <[brasil.elpais.com](http://brasil.elpais.com)>

**Feynman** estudou no *Massachusetts Institute of Technology* onde obteve seu B. Sc. (1939) e na *Princeton University* onde obteve seu Ph.D. (1942). Foi *research assistant* em Princeton (1940-1941), professor of Theoretical Physics na *Cornell University* 1945-1950), visiting professor e, professor of Theoretical Physics no *California Institute of Technology* (1950-1959 ). **Feynman** foi membro da *American Physical Society* e da *National Academy of Science*, foi também eleito membro estrangeiro da *Royal Society*, London (1965). Além do Nobel recebeu várias outras honrarias como

o *Albert Einstein Award* (1954, Princeton) e a *Lawrence Award* (1962). **Richard Feynman** (1982) foi um passo mais perto de um verdadeiro computador quântico com seu simulador "quantum universal". A ideia consistiu em um "lattice of spin systems" livremente especificável. Embora, possa certamente simular qualquer sistema com um espaço de estados de dimensão finita, **Deutsch** não entendeu porque **Feynman** duvidou que pudesse simular sistemas de *férmions*, não é uma máquina no sentido deste artigo. 'Programação' o simulador consiste em dotá-lo com as leis dinâmicas desejadas e, em seguida, colocá-lo em um estado inicial desejado. Mas o mecanismo que permite selecionar leis dinâmicas arbitrárias não é modelado. A dinâmica de um verdadeiro "computador quântico", imaginado por **Deutsch**, deve ser dada de uma vez por todas, e a programação deve consistir inteiramente em prepará-lo em um estado adequado.

Adicionalmente a seus trabalhos sobre física teórica, **Feynman** foi pioneiro na área de computação quântica, introduzindo o conceito de *nanotecnologia*, no encontro anual da *Sociedade Americana de Física*, em 29 de dezembro de 1959, em sua palestra sobre o controle e manipulação da matéria em escala atômica, embora não tenha utilizado este termo em sua palestra, onde apresentou pela primeira vez suas ideias acerca do assunto. Defendeu a hipótese de que não existe qualquer obstáculo teórico à construção de pequenos dispositivos compostos por elementos muito pequenos, no limite atômico, nem mesmo o *princípio da incerteza*. A *nanotecnologia* é uma ciência que se dedica ao estudo da manipulação da matéria numa escala atômica e molecular lidando com estruturas entre 1 e 1000 nanômetros. A palavra "*nanotecnologia*" foi utilizada pela primeira vez pelo professor **Norio Taniguchi** em 1974 para descrever as tecnologias que permitam a construção de materiais a uma escala de 1 nanômetro ( $10^{-9}$  metro). Para se perceber o que isto significa, considere uma praia de 1000 km (1.000.000.000 mm) de extensão e um grão de areia de 1 mm, este grão está para esta praia como um nanômetro está para o metro. Nanotecnologia pode ser utilizada em diferentes áreas como, a medicina, eletrônica, ciência da computação, física, química, biologia e engenharia dos materiais.

**David Z. Albert** (1983) (Figura 134) - É professor de Filosofia e Diretor do Programa M.A. em *The Philosophical Foundations of Physics* na *Columbia University* em New York. **Albert** descreveu uma medida na mecânica quântica (baseada num "autômato") e observou que suas propriedades ao serem ajustadas para se medir (**ALBERT**, 1983), não têm análogo entre os autômatos clássicos. Os autômatos de **Albert**, embora não sejam máquinas de computação de propósito geral, são verdadeiros computadores quânticos, membros da classe geral, como estudada no artigo "*Quantum theory, the Church-Turing principle and the universal quantum computer*" (**DEUTSCH**, 1985).

Em 1989, **Deutsch** introduziu o modelo de circuitos quânticos (**DEUTSCH**, 1989), e isto fez crescer ainda mais o interesse em computação quântica.

O algoritmo de **Deutsch** reescrito na nova linguagem (*qubits*) (1992) teve, então, uma ampla repercussão, pois a linguagem dos *qubits* (análogo quântico ao bit clássico) abriu um paralelismo entre a linguagem de circuitos quânticos e os digitais clássicos. Após as ideias precursoras que levaram à noção de computadores quânticos, **David Deutsch**, em 1985 (**DEUTSCH**, 1985), publicou a primeira proposta teórica para um algoritmo onde se faz uso explícito do paralelismo computacional que surge do princípio da superposição de estados quânticos, na resolução de um

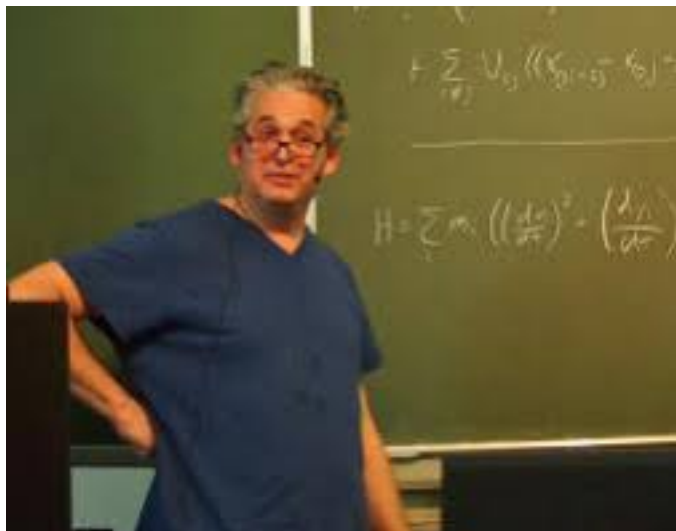


Figura 134 – David Albert - descreveu uma medida na mecânica quântica, baseada num autômato.

Fonte: <<https://www.mathematik.uni-muenchen.de>>

problema matemático específico sobre funções binárias. Este foi o primeiro algoritmo quântico a ser criado, e demonstrou o poder da computação quântica sobre a clássica, pois resolve um problema utilizando um método que não possui análogo clássico.

Em 1994 surgiu o trabalho que fez eclodir o interesse por computação quântica, publicado por **Peter Shor**. Neste artigo, **Shor** propõe um esquema para fatoração de números grandes com ganho exponencial de tempo, quando comparado com algoritmos clássicos. O algoritmo de **Shor** é uma evidência de que o modelo computacional quântico proposto pode superar de fato o modelo clássico derivado das máquinas de **Turing**. O resultado de **Shor** impulsionou a pesquisa por sistemas físicos onde estas ideias pudessem ser implementadas, objetivando a construção de um computador que funciona sujeito às leis da física quântica, ou melhor, utilizando suas extraordinárias propriedades.

Em 1996, **Lov Grover** publicou um outro trabalho de grande importância, onde reporta a criação de um algoritmo quântico de busca em listas desordenadas, que é quadraticamente mais rápido do que seus análogos clássicos. Os trabalhos de **Shor** e **Grover** são frequentemente citados como os dois grandes motivadores para estudos em computação quântica, pois estes são demonstrações comprovadas do poder da computação quântica sobre a clássica. Estes estudos justificam as pesquisas por mais algoritmos quânticos, por dispositivos e materiais capazes de serem utilizados como chips quânticos e também por técnicas experimentais capazes de manipular os estados quânticos dos *qubits* com alta precisão.

Estes algoritmos quânticos serão abordados no capítulo 11.

## 10.4 Os princípios do computador quântico

Este capítulo está baseado no trabalho de **Hamilton José Brumatto**, *Introdução à Computação Quântica* (BRUMATTO, 2012).

A evolução dos computadores, de hoje, está limitada por duas barreiras inatingíveis para o modelo atual: **velocidade da luz** no processamento da informação e a dimensão da ordem de grandeza atômica, no tamanho dos componentes em um *chip*.

A Computação Quântica é a continuidade natural na evolução dos computadores para fisicamente tentar atingir estas barreiras. O *Princípio da Incerteza* associado à *estrutura quântica da matéria* define um mecanismo para que computadores quânticos implementem uma *máquina probabilística de Turing*. Assim, os computadores quânticos poderão ser utilizados na solução de problemas intratáveis da classe *NP-completo* <<https://pt.wikipedia.org/wiki/NP-completo>>. É possível definir bits quânticos, ou *qubits*, para representação da informação e construir um conjunto universal de *portas quânticas* para operar sobre os *qubits*, seguindo uma programação pré-definida. Alguns protótipos já demonstram a implementação da computação quântica, no entanto, são apenas modelos experimentais. Assim, a computação quântica apresenta uma perspectiva positiva de futuro.

A Lei de **Moore Moore (1965)** traz uma predição que tem se confirmado nos últimos anos (HENNESSY; PATTERSON, 2008), no entanto não é possível que a taxa de crescimento predita ou medida se mantenha, e isto é evidenciado por uma quebra mais recente no ritmo do crescimento (HENNESSY; PATTERSON, 2008). Um dos motivos da dificuldade de manter o crescimento é que o aumento do número de componentes em um chip implica na diminuição do tamanho de cada componente, neste caso, se a taxa de crescimento se mantiver teremos componentes atingindo o tamanho de um átomo, o que é uma situação impossível. Outro fator a se considerar é o limite na solução de problemas computacionais que a arquitetura concebida no modelo da Máquina de Turing oferece, por mais rápido que sejam as máquinas ainda não é possível resolver problemas considerados *NP-completos* (MOORE, 1965) para uma entrada suficientemente grande. Conclui-se então que há a necessidade de se criar um novo paradigma na construção de hardware.

Uma máquina probabilística de **Turing** (CORMEN et al., 2001) é suficiente para resolver problemas definidos *NP-completos* em tempo polinomial. Com base nesta ideia, **David Deutsch** procurou definir um dispositivo computacional capaz de simular eficientemente sistemas físicos arbitrários (NIELSEN; CHUANG, 2000) como base para a construção de uma máquina probabilística. Como esses sistemas físicos são basicamente ditados pela mecânica quântica, surgiu a proposta inicial de construção de computadores quânticos. Esta ideia tem sido desenvolvida até a concepção moderna da computação quântica.

A base da computação quântica é a representação de um bit quântico, o *qubit*. De forma análoga a um sistema computacional clássico, é necessário um sistema quântico que apresente um *qubit* com dois estados bem definidos, que serão indicados por  $|0\rangle$  e  $|1\rangle$ . apesar de possuir estes dois estados quânticos fundamentais, o sistema utilizado poderá se encontrar em um estado que é na realidade uma *sobreposição* dos estados fundamentais. A *sobreposição* é indicada por uma *distribuição probabilística através dos estados fundamentais*. Um *estado do sistema* fica, então, descrito por um vetor, no qual cada posição desse vetor está associada a um estado fundamental e o

valor representado define a probabilidade do *qubit* estar naquele estado fundamental. Em um sistema com  $n$  *qubits* teremos  $2^n$  estados fundamentais possíveis. Ao medir o sistema obtemos um único valor que indica apenas o conjunto de estados fundamentais nos quais cada *qubit* do sistema se encontra. O estado medido segue uma distribuição probabilística. Este mecanismo é a base de concepção de uma *máquina probabilística de Turing*.

Uma arquitetura de um sistema quântico pode ser construída de forma semelhante à arquitetura clássica: **Memória**, **ULA** (Unidade Lógica e Aritmética) e **Circuito de Controle**. **Memória** e **ULA** serão dispositivos quânticos, o **Circuito de Controle** pode possuir uma interface na computação clássica para gerenciar o controle de fluxo quântico e mecanismos de correção de erros. A ULA poderia ser construída através de um conjunto universal de portas lógicas quânticas. Algumas propriedades físicas têm sido exploradas para implementar uma máquina real, no entanto os protótipos ainda trabalham com cerca de uma centena de *qubits*, o que pode ser ainda insuficiente para qualquer resultado prático.

## 10.5 A incerteza por princípio

A Física clássica é fundamentada pela descrição dos movimentos dos corpos introduzida por **Isaac Newton** (NEWTON, 1999), e também pela descrição do comportamento dos campos e ondas eletromagnéticas compilada por **James Clerk Maxwell** (MAXWELL, 1954). As várias teorias, teoremas e experimentos construídos ao longo dos últimos séculos pelos sucessores e até mesmo antecessores de **Newton** e **Maxwell** demonstraram que as equações da mecânica e do eletromagnetismo descrevem com grande sucesso os fatos observados. No início do século passado, alguns experimentos ficaram inexplicados: por exemplo, pela *teoria do eletromagnetismo*, um elétron quando acelerado emite energia na forma de radiação eletromagnética e com isto, baseado no *princípio da conservação da energia*, diminui sua própria energia de movimento, e decorrente disto um elétron submetido à ação de uma força (aceleração) centrípeta em um movimento ao redor do núcleo deve perder sua energia e se precipitar no núcleo, o que não ocorre.

Outras contradições entre fatos reais/experimentais e previsões teóricas surgiram, entre eles um famoso problema, a catástrofe do ultravioleta de **Rayleigh** e **Jeans** (EKERT; HAYDEN; INAMORI, 2001). O problema considera que um corpo negro teria uma energia infinita, e a energia é função da temperatura e da frequência da radiação eletromagnética. Dada uma frequência, a energia obtida é uma integral em um intervalo contínuo e isto faz com que esta integral resulte em valor infinito, quando calculada para frequências na região do ultravioleta. **Max Planck** resolveu este problema, ele propôs que a energia não assuma valores contínuos, e sim múltiplos de um valor mínimo:  $E = n.h.f$ , sendo  $f$  a frequência,  $h$  uma constante (constante de **Planck**) e  $n$  valores inteiros. O valor mínimo possível,  $E = h\nu$  é o *quanta* de energia. Com isto a energia total passou a ser uma soma discreta e não mais uma integral, coerente com os resultados experimentais. Com a definição do *quanta de energia*, os valores de energia possíveis são quânticos". Este foi o primeiro trabalho que deu início à Física Quântica.

**Heisenberg** (HEISENBERG, 1949) em seu trabalho sobre princípios da teoria quântica, trouxe uma compilação de vários experimentos que apresentava a ambiguidade entre a natureza corpuscular e ondulatória da matéria. Por exemplo, raios  $\beta$  ao

passarem por uma câmara de bolhas deixam um rastro compatível com a natureza de uma partícula, é possível determinar massa e velocidade. Por outro lado, os raios  $\beta$  ao atravessarem um filme fino de material cristalino formam uma figura de difração em um anteparo, compatível com a natureza de uma onda, é possível medir sua frequência. Isto significa que um feixe de raios pode ser descrito, tanto como uma frente de onda, quanto como um conjunto de partículas. O mesmo foi observado para os raios X, que como são radiações eletromagnéticas, possuem a natureza de onda. Quando um feixe deste raio atravessa um vapor supersaturado de água, é deixado um rastro tal qual um conjunto de partículas, também se observa o efeito de difração para o raio X. Decorrente da natureza dual partícula-onda **Heisenberg** deduziu que o conhecimento da posição de uma partícula com a precisão  $\Delta x$  e o conhecimento do momento (velocidade) da partícula com a precisão  $\Delta p$  deve obedecer o limite:  $\Delta x \cdot \Delta p > h/(4\pi)$ , sendo  $h$  a constante de **Planck**. Este resultado é conhecido como o *Princípio de Incerteza* de **Heisenberg**, e deriva diretamente da dualidade partícula-onda, não é possível conhecer simultaneamente a posição e velocidade de uma partícula, exceto dentro de um limite de incerteza, que é pequeno comparado ao valor da massa de corpos do nosso cotidiano, mas é expressivo em um mundo subatômico.

Enquanto realizava experiências para evidenciar a dualidade partícula-onda também para a luz, que é uma forma de radiação eletro-magnética, **Eisntein** demonstrou através do efeito foto-elétrico, o que lhe valeu um prêmio Nobel, que a luz também pode ser interpretada na forma de partícula, chamada fóton. Com base nisso propôs-se uma experiência na obtenção de figuras de difração a partir de fótons (RAE, 1986). Nesta experiência emite-se luz com intensidade bem baixa, quase que um fóton por vez, de forma a passar por um anteparo com dois furos, observa-se que no resultado, cada fóton imprime uma imagem que compõe ao longo do tempo, com a imagem de outros fótons, a figura da difração, isto indica que a natureza onda do fóton permite que este, mesmo sendo uma única partícula, atravesse ao mesmo tempo ambos furos formando a figura de difração, e cada fóton acaba sendo impresso como um ponto, ou partícula, no anteparo. Se for colocado um tipo de detecção, logo na saída dos furos para identificar por qual furo o fóton passa, de fato, observa-se que cada fóton passa por um único furo, e no entanto perde-se a figura de difração. A medida da posição ou velocidade do fóton afeta seu estado.

*O princípio da incerteza e o resultado de que uma medida afeta o estado de uma partícula nos limites quânticos nos permitirá entender o modelo da computação quântica.*

## 10.6 Bits e quBits

Diversos itens são aqui descritos no que diz respeito a *bits* convencionais e bits quânticos, os *qubits*. Veja na Figura 135 um visão comparativa entre um computador clássico e um computador quântico.

- A unidade básica de informação em computadores digitais é o *bit*. Um *bit* pode ter os valores lógicos "0" ou "1".
- Nos computadores digitais, um *bits* é fisicamente representado pela presença ou não de correntes elétrica em componentes eletrônicos dentro dos chips: a

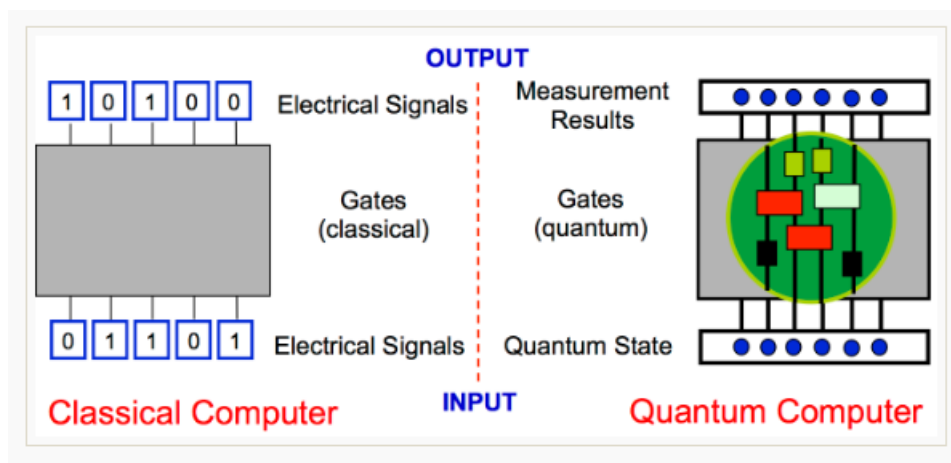


Figura 135 – Visão comparativa entre um computador clássico e um quântico.

Fonte: <[http://qoqms.phys.strath.ac.uk/research\\_qc.html](http://qoqms.phys.strath.ac.uk/research_qc.html)>

presença da corrente indica o estado lógico 1 e a sua ausência o estado lógico 0. Portanto, os dois valores lógicos de um bit são *mutuamente excludentes*.

- Um computador clássico tem uma memória feita de bits. Cada bit guarda um "1" ou um "0" de informação. Um computador quântico mantém um conjunto de *qubits*. Um *qubit* pode conter um "1", um "0" ou uma sobreposição destes. Em outras palavras, pode conter tanto um "1" como um "0" ao mesmo tempo. O computador quântico funciona pela manipulação destes *qubits*.
- Em outras palavras, a unidade de informação quântica é o bit quântico, ou *qubit* (do inglês **q**uantum **b**inary **d**igit), o qual pode assumir os valores lógicos "0", "1" ou qualquer *sobreposição* destes.
- Fisicamente, um *qubit* é representado por qualquer objeto quântico que possua dois estados bem distintos, como estados de polarização de um *fóton* ou as orientações de *spins* nucleares.
- Os estados quânticos de 1 *qubit* são representados por  $|0\rangle$  e  $|1\rangle$ . A **sobreposição quântica** é um dos princípios fundamentais da mecânica quântica (AZAMBUJA, 2016) que afirma que:

*Um sistema físico existe parcialmente em todos os estados teoricamente possíveis, simultaneamente, antes de ser medido. Porém quando medido ou observado, o sistema se mostra em um único estado. Como representar tais superposições? A notação utilizada na computação quântica são para esses casos, como:  $|0\rangle$  ou  $|1\rangle$  ou  $|01\rangle$  ou  $|10\rangle$ .*

O conceito dos bits quânticos, em (EKERT; HAYDEN; INAMORI, 2001), leva em consideração estados quânticos da matéria. Um bit quântico pode ser representado por um sistema quântico que possua dois estados fundamentais, que podem ser indicados como  $|0\rangle$  ou  $|1\rangle$ <sup>2</sup>. Se um sistema for medido no

<sup>2</sup> A notação apresentada é a notação *bra-ket* definida por Paul Dirac para representação de estados quânticos (DIRAC, 1939).



estado representado como  $|0\rangle$ , então não está no estado  $|1\rangle$ . No entanto, os estados quânticos que um sistema pode, não necessariamente, recair em um ou outro estado fundamental, o **Princípio da Incerteza** nos diz que há uma *probabilidade* de o sistema **simultaneamente** estar em um ou outro estado fundamental, um determinado estado que pode ser representado de acordo com esta probabilidade como:

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

Como os estados são representados por vetores ortogonais, devemos ter  $\alpha^2 + \beta^2 = 1$ , e  $\alpha^2$  e  $\beta^2$  representam as probabilidades do sistema estar em um ou outro estado. Um conceito mais geral considera estas constantes como números complexos, como nos espaços vetoriais de **Hilbert** sobre  $\mathbb{C}$ .

- Um sistema quântico composto por vários *qubits* também é chamado de *registrator quântico*. Na essência, um computador quântico manipula a informação, como se os quatro estados quânticos provenientes dos dois **qubits** existissem ao mesmo tempo, e essa propriedade torna possível uma capacidade computacional muito além da que temos acesso na atualidade. Um *computador quântico* é um dispositivo que executa cálculos, fazendo uso direto de propriedades da mecânica quântica, tais como *sobreposição*, *interferência* e o *princípio da incerteza*.

## 10.7 O uso da probabilidade

O uso da **probabilidade** nos cálculo da Física deu excelente resultado, levando a uma ampliação dos horizontes do conhecimento e a inventos como a televisão e o raio laser. Mas a *probabilidade* também tem as suas limitações e, quando aplicada a uma teoria fundamental, como é o caso da mecânica quântica, provoca certa inquietação. Uma coisa, por exemplo, é alguém olhar um carro e dizer: "A velocidade daquele carro é de 100 quilômetros por hora". Outra, bem diferente, é dizer: "Aquele carro não tem velocidade definida; é provável que seja 100 quilômetros por hora, mas também pode ser 80 ou 120". Nas duas situações, existem informações básicas sobre o carro - calcular a velocidade é um dado fundamental para qualquer teoria física. Mas, na primeira, a informação é inequívoca: um único número. Em lugar disso, a **resposta probabilística** fornece um conjunto de números, como se o carro pudesse desenvolver diversas velocidades ao mesmo tempo. Do ponto de vista científico, as respostas múltiplas da mecânica quântica significam apenas isso: **a teoria, em certos casos, oferece um conjunto de resultados mais ou menos prováveis para determinado cálculo**. Qualquer interpretação além disso é simples imaginação. Um problema é que, no caso de um corpo como o carro, a Física sempre dá uma resposta única e taxativa - **a probabilidade só afeta os corpos microscópicos**. Esse fato força uma divisão do mundo físico em duas partes, numa das quais valem **leis probabilísticas e deterministas**, e no outro, apenas *leis probabilísticas*. Atualmente, a grande maioria dos cientistas aceita as equações probabilísticas.

## 10.8 Entendendo estados quânticos com dois qubits

Agora, se estivéssemos trabalhando com a computação clássica, com os dois bits convencionais "0" e "1", teríamos quatro estados possíveis:  $\{00, 01, 10, 11\}$ . Se

forem **quatro estados clássicos** poderão representar **dois qubits** simultâneos em seus estados fundamentais representados como  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ .

Para a manipulação dos *estados quânticos* com **dois qubits**, utiliza-se o seguinte raciocínio: suponhamos agora que temos dois **qubits**, como consequência, temos que um sistema quântico, com dois *qubits* possuindo quatro estados quânticos representados na base computacional:  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ .

Contudo, de acordo com o **princípio da superposição**, exemplificado por **Schrödinger**, como um par de *qubits* também pode existir, para um determinado instante de tempo, em superposições destes estados, então obtêm-se coeficientes complexos associados a cada um dos estados - associa-se uma *amplitude de probabilidade* ao estado genérico  $|\psi\rangle$ . Dessa forma pode-se representar o vetor de *estado quântico* genérico como:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

onde os coeficientes  $\alpha_{00}$ ,  $\alpha_{01}$ ,  $\alpha_{10}$  e  $\alpha_{11}$  são números complexos, onde

$$\sum_{x \in \{0,1\}^2} |\alpha_x|^2 = 1 \text{ (condição de normalização),}$$

sendo úteis nos cálculos de probabilidades.

Similarmente ao caso para um *qubit* só, o resultado da medição de  $x$  ocorre com probabilidade  $|\alpha_x|^2$ , resultando no estado  $|x\rangle$ .

Pode-se, também, medir apenas um subconjunto dos *qubits*; o resultado é similar: medir o primeiro *qubit* resultaria em 0 com probabilidade  $|\alpha_{00}|^2 + |\alpha_{01}|^2$ , resultando no estado de pós-medição:

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Note como  $|\psi'\rangle$  é renormalizado para ter comprimento unitário.

Este conceito pode se expandir a sistemas quânticos que apresentem vários estados fundamentais, e o sistema poderá estar em uma distribuição probabilística sobre esses estados, para descrever um estado genérico  $|\psi\rangle$ .

Para tratar da unidade básica de informação em computadores quânticos, é necessário recorrer ao conceito de espaço de **Hilbert** e da *Esfera de Bloch*.

Um espaço de **Hilbert** ( $\mathcal{H}$ ) é um espaço vetorial complexo provido de uma métrica dada por um produto escalar. Em um espaço vetorial  $\mathcal{H}$ , uma combinação linear de dois elementos pertencentes a  $\mathcal{H}$ ,  $|\psi_1\rangle$  e  $|\psi_2\rangle$ , também pertence a  $\mathcal{H}$ , ou seja, dados  $|\psi_1\rangle \in \mathcal{H}$  e  $|\psi_2\rangle \in \mathcal{H}$ , então  $a|\psi_1\rangle + b|\psi_2\rangle \in \mathcal{H}$ , onde  $a$  e  $b$  são números complexos.

Sendo os estados de um *qubit* são representados por  $|0\rangle$  e  $|1\rangle$ . O conjunto desses estados  $\{|0\rangle, |1\rangle\}$  forma uma base no espaço de **Hilbert** de duas dimensões, tal que:

Tabela 1 – Pontos especiais sobre a Esfera de Bloch

$\theta$	$\varphi$	$ \psi\rangle$	Comentário
0	0	$ 0\rangle$	Polo Norte
$\pi$	0	$ 1\rangle$	Polo Sul
$\frac{\pi}{2}$	0	$( 0\rangle +  1\rangle)/\sqrt{2}$	Equador, sobre o eixo x
$\frac{\pi}{2}$	$\frac{\pi}{2}$	$( 0\rangle + j 1\rangle)/\sqrt{2}$	Equador, sobre o eixo y

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

O estado genérico (sobreposição de estados) de um *qubit* é representado por:  $|\psi\rangle = a|0\rangle + b|1\rangle$ , onde  $a$  e  $b$  são números complexos tais que  $|a|^2 + |b|^2 = 1$ .

Este estado genérico pode ser parametrizado por ângulos  $\theta$  e  $\varphi$ , fazendo-se:

$$a = \cos\left(\frac{\theta}{2}\right) \text{ e } b = \exp(j\varphi) \cdot \sin\left(\frac{\theta}{2}\right),$$

o que produz:

$$|\psi\rangle = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) \\ \exp(j\varphi) \cdot \sin\left(\frac{\theta}{2}\right) \end{bmatrix} |0\rangle + \begin{bmatrix} \exp(j\varphi) \cdot \sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) \end{bmatrix} |1\rangle$$

Esta representação permite que o estado de um *qubit* corresponda a um ponto sobre a superfície de uma esfera. Tal esfera é chamada de *Esfera de Bloch*, a qual é apresentada nas Figuras 136, 137:

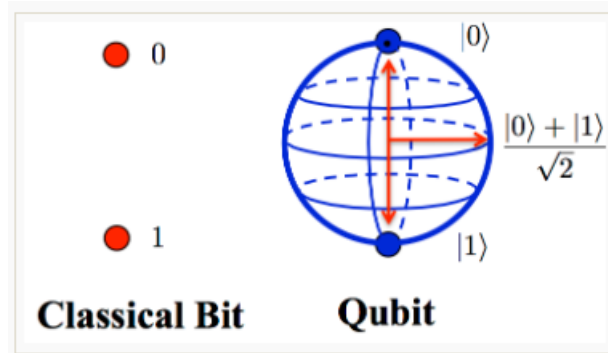


Figura 136 – Visão comparativa entre o bit clássico e um bit quântico (qubit).

Fonte: <[http://qoqms.phys.strath.ac.uk/research\\_qc.html](http://qoqms.phys.strath.ac.uk/research_qc.html)>

Pontos especiais sobre a *esfera de Bloch* são mostrados na Tabela 1:

Fica evidenciado, portanto, que um único *qubit* pode armazenar uma, dentre infinitas informações, que são todas as combinações lineares possíveis dos números complexos  $a$  e  $b$ , sempre respeitando  $a^2 + b^2 = 1$ . Essas combinações lineares são chamadas de **superposições dos auto-estados**.

Não importando em que estado de superposição se encontre um *qubit*, a leitura

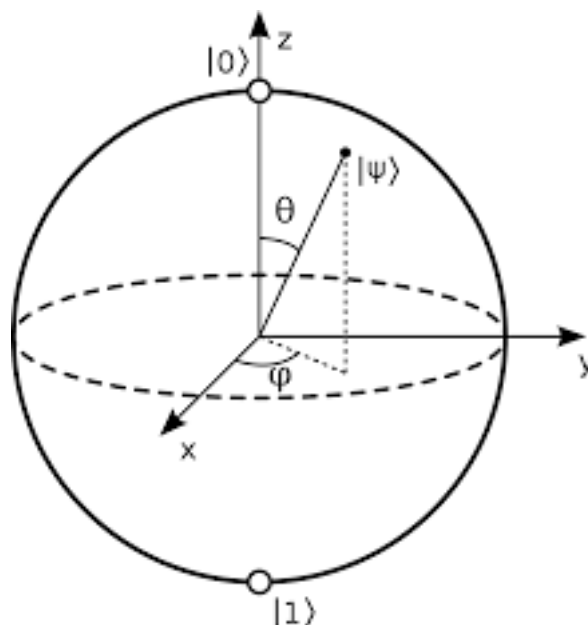


Figura 137 – Esfera de Bloch.

Fonte: IA013 - Introdução à Computação Natural - Prof. Fernando J. Von Zuben, DCA/FEEC/Unicamp.

de seu valor será sempre  $|0\rangle$  ou  $|1\rangle$ . Isso ocorre porque a leitura promove o *colapso do estado para um dos auto-estados*.

O estado do *qubit* vai colapsar em  $|0\rangle$  com probabilidade  $a^2$  ou vai colapsar em  $|1\rangle$  com probabilidade  $b^2$ .

O Espaço de **Hilbert** de dois *qubits* é expandido pelos vetores formados pelo *produto tensorial*:

$$\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

A representação desses *auto-estados* (estados fundamentais) é dada por:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}; \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}; \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}; \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Ao trabalhar com sistemas que possuam dois qubits, um qubit estará no estado  $|\psi\rangle$  e o outro no estado  $|\phi\rangle$ , cada qual representado por uma distribuição probabilística: com isso teremos no final uma sobreposição probabilística desses estados genéricos, representando o estado do sistema quântico, pelo produto tensorial de um espaço de Hilbert, tal que:

A última linha da equação acima apresenta uma notação mais simples para os estados fundamentais quânticos em sistemas com dois qubits. Fica claro que um sistema quântico que apresenta quatro estados fundamentais pode ser representar um sistema

$$\begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \text{ e} \\ |\phi\rangle &= \eta|0\rangle + \delta|1\rangle \end{aligned}$$

Figura 138 – Dois estado quânticos genéricos  $|\psi\rangle$  e  $|\phi\rangle$ .

Fonte: (BRUMATTO, 2012)

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= |\psi\rangle |\phi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\eta|0\rangle + \delta|1\rangle) \\ &= \alpha\eta(|0\rangle \otimes |0\rangle) + \alpha\delta(|0\rangle \otimes |1\rangle) \\ &\quad + \beta\eta(|1\rangle \otimes |0\rangle) + \beta\delta(|1\rangle \otimes |1\rangle) \\ &= \alpha\eta|00\rangle + \alpha\delta|01\rangle + \beta\eta|10\rangle + \beta\delta|11\rangle \\ &= \alpha\eta|1\rangle + \alpha\delta|2\rangle + \beta\eta|3\rangle + \beta\delta|4\rangle \quad (3.4) \end{aligned}$$

Figura 139 – Produto tensorial de dois estados quânticos genéricos  $|\psi\rangle$  e  $|\phi\rangle$ .

Fonte: (BRUMATTO, 2012)

com dois qubits. Outro detalhe na equação acima é a *linearidade*, isto é possível, pois os estados são bem descritos por um vetor, ou seja, os estados  $|0\rangle$  e  $|1\rangle$  são ambos auto-vetores (vetores da base do espaço vetorial  $\mathcal{H}$ ) que representam soluções possíveis para um estado quântico:

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

Figura 140 – Um vetor de estado quântico genérico  $|\psi\rangle$ .

Fonte: (BRUMATTO, 2012), as equações (3.5)

Pode-se representar o produto tensorial de desta forma:

$$|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \eta \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha\eta \\ \alpha\delta \\ \beta\eta \\ \beta\delta \end{bmatrix}$$

Figura 141 – Um produto tensorial de estados genéricos  $|\psi\rangle$  e  $|\phi\rangle$ .

Fonte: (BRUMATTO, 2012), as equações (3.6)

Prosseguindo com este raciocínio, conclui-se que um computador quântico com  $n$  qubits em superposição vai ter  $2^n$  auto-estados. Este conceito pode ser generalizado a sistemas quânticos que apresentem vários estados fundamentais, e o sistema quântico

poderá ter uma distribuição probabilística sobre esses estados.

Dada a *linearidade*, quando realizamos uma medida no sistema acima em apenas um *qubit*, o *qubit* seguinte pode se apresentar em qualquer outro estado. Feita a medida, e supondo que o primeiro bit se encontra no estado  $m$ ,  $m \in \{0, 1\}$ , o estado resultante é:

$$|\Psi\rangle = \eta|m, 0\rangle + \delta|m, 1\rangle$$

Figura 142 – Linearidade quando apenas um qubit de dois qubits é medido.

Fonte: (BRUMATTO, 2012), equações (3.7)

isto é, medindo apenas 1 qubit, o outro qubit poderá estar em qualquer outro estado.

Porém, nem todos os estados podem ser descritos por uma combinação linear de dois estados separados. Considere o estado representado pela equação:

$$|\Psi\rangle = \eta|0, 0\rangle + \delta|1, 1\rangle$$

Figura 143 – Quando a medida de dois qubits não é feita separada.

Fonte: (BRUMATTO, 2012), equações (3.8)

uma vez feita a leitura do primeiro *qubit*, no estado  $m$ , o segundo *qubit*, necessariamente, estará no mesmo estado  $m$ . Este estado é conhecido como **Estado de Bell**, e **este estado não é atingível por uma combinação linear de estados individuais dos qubits**. O Estado de Bell ou também conhecido como o par EPR (Einstein, Podolsky e Rosen) - porque estamos considerando dois estados genéricos medidos juntos - apresenta correlações fortes, maiores que quaisquer outras que poderiam existir em sistemas clássicos (NIELSEN; CHUANG, 2000). Este estado é a chave para o **teleporte-quântico** que falaremos mais à frente.

Se considerarmos um sistema com  $n$  qubits, teremos um estado final que é a junção dos vários estados individuais  $i$ , conforme vemos na equação abaixo, além dos Estados de Bell para o sistema de múltiplos qubits medidos juntos. Os estados possíveis do sistema crescem de forma exponencial.

As operações em um computador quântico ocorrem através de **portas quânticas** sobre estados quânticos do sistema, as medidas são obtidas com base na distribuição probabilística na descrição de cada estado quântico genérico. A partir do momento que temos um conjunto de medidas sobre a distribuição probabilística nos estados genéricos do sistema, podemos intuir que um computador baseado em sistemas quânticos representa uma implementação da máquina probabilística de **Turing** (OMER, 2000) e (OMER, 2009). Em *Teoria da Computabilidade*, uma *máquina de Turing probabilística* é uma máquina de **Turing** não determinística que escolhe aleatoriamente dentre as transições a cada ponto, de acordo com alguma *distribuição de probabilidade* <[https://pt.wikipedia.org/wiki/Máquina\\_de\\_Turing\\_probabilística](https://pt.wikipedia.org/wiki/Máquina_de_Turing_probabilística)>.

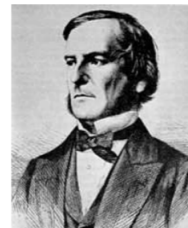
$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes \dots \otimes |\psi_n\rangle$$

Figura 144 – A medida do estado genérico do sistema quântico corresponde ao produto tensorial dos estados genéricos individuais de cada qubit.

Fonte: (BRUMATTO, 2012), equações (3.9)

## Histórico

- Em meados do século XIX o matemático inglês **George Boole** desenvolveu um sistema matemático de análise lógica
- Em meados do século XX, o americano Claude Elwood **Shannon** sugeriu que a Álgebra Booleana poderia ser usada para análise e projeto de circuitos de comutação



George Boole (1815-1864)



Claude Elwood Shannon (1916-2001)

Figura 145 – Histórico das portas lógicas clássicas.

Fonte:

<<http://dcm.ffclrp.usp.br/~augusto/teaching/aba/AB-Funcoes-Logicas-Portas-Logicas.pdf>>

### 10.9 Portas lógicas clássicas

As portas lógicas clássicas podem operar na entrada, 1 bit (chamadas operações unárias) ou sobre 2 bits (operações binárias). É possível estender o conceito de uma porta lógica operar sobre um número qualquer de bits de entrada.

### 10.10 Portas lógicas quânticas

Na teoria da informação quântica, um *circuito quântico* é um modelo para a computação quântica em que uma computação é uma sequência de *portas quânticas*, que são transformações reversíveis em um registrador quântico de n-qubits.

Tal como na computação clássica, as portas lógicas devem operar sobre bits de entrada gerando bits na saída, a diferença é que na computação quântica as portas devem operar sobre estados quânticos. Podemos definir uma *porta lógica quântica* como um dispositivo que consegue realizar, em um período finito de tempo, uma operação unitária definida em um conjunto específico de qubits (EKERT; HAYDEN;

## Álgebra Booleana

---

- ❑ Na álgebra de Boole, há somente dois **estados** (**valores** ou **símbolos**) permitidos
    - Estado **0** (zero)
    - Estado **1** (um)
  - ❑ Em geral
    - O estado zero representa **não**, **falso**, aparelho desligado, ausência de tensão, chave elétrica desligada, etc
    - O estado um representa **sim**, **verdadeiro**, aparelho ligado, presença de tensão, chave ligada, etc
- 

Figura 146 – Os valores lógicos na Álgebra Booleana.

Fonte:

<<http://dcm.ffclrp.usp.br/~augusto/teaching/aba/AB-Funcoes-Logicas-Portas-Logicas.pdf>>

## Álgebra Booleana

---

- ❑ Assim, na álgebra booleana, se representarmos por 0 uma situação, a situação contrária é representada por 1
  - ❑ Portanto, em qualquer bloco (porta ou função) lógico somente esses dois estados (0 ou 1) são permitidos em suas entradas e saídas
  - ❑ Uma variável booleana também só assume um dos dois estados permitidos (0 ou 1)
- 

Figura 147 – Os valores lógicos na Álgebra Booleana.

Fonte:

<<http://dcm.ffclrp.usp.br/~augusto/teaching/aba/AB-Funcoes-Logicas-Portas-Logicas.pdf>>



# Álgebra Booleana

---

- Nesta apresentação trataremos dos seguintes blocos lógicos
    - E (AND)
    - OU (OR)
    - NÃO (NOT)
    - NÃO E (NAND)
    - NÃO OU (NOR)
    - OU EXCLUSIVO (XOR)
  - Após, veremos a correspondência entre expressões, circuitos e tabelas verdade
  - Por último, veremos a equivalência entre blocos lógicos
- 

Figura 148 – Os valores lógicos na Álgebra Booleana.

Fonte:

<http://dcm.ffclrp.usp.br/~augusto/teaching/aba/AB-Funcoes-Logicas-Portas-Logicas.pdf>

(INAMORI, 2001).

Por motivos de prática de engenharia, normalmente estuda-se portas apenas para valores pequenos de  $n$ , ou seja  $n=1$ ,  $n=2$  ou  $n=3$ . Estas portas podem ser facilmente descritas por tabelas.

## 10.11 Portas de 1 qubit

Portas quânticas unárias (que operam sobre um único qubit) são representadas por matrizes  $2 \times 2$  unitárias, sendo capazes apenas de rotacionar o *qubit* na esfera de **Bloch**, levando o *qubit* a um outro estado de sobreposição. **Esta é a razão pela qual toda porta quântica é reversível.**

A Figura 1 apresenta um diagrama para a porta NOT (NÃO) incluindo a tabela verdade que indica a saída conforme a entrada. Esta é a única porta lógica reversível de um computador clássico. Na tabela-verdade que indica a saída conforme a entrada: se entra 0, sai 1 e vice-versa, se entra 1, sai 0. Esta é, a porta NOT de saída binária.

### 10.11.1 Porta NOT quântica

O que esperamos para uma porta NOT quântica é a capacidade de, dado um estado quântico fundamental como entrada, resultar no estado quântico inverso. Se esta porta operar sobre o estado  $|0\rangle$  devemos obter como saída o estado  $|1\rangle$  e também o inverso. **Como os estados quânticos são representados por uma notação vetorial**



## Porta *NÃO* da lógica binária

Figura 149 – Porta NOT da lógica binária.

Fonte: Introdução à Computação Quântica, Hamilton José Brumatto, UNICAMP.

(ou seja, podem ser representados por vetores), **os operadores que modificam estes estados são representados por matrizes.**

### 10.11.2 Porta CNOT quântica

A porta CNOT quântica, chamada de Porta  $X$  (que troca o bit quântico) 150, quando aplicada sobre o estado  $|0\rangle$  resulta no estado  $|1\rangle$  e vice-versa. O uso da porta  $X$  pode ser visto na equação 151.

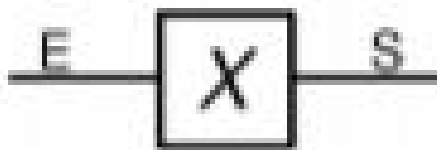


Figura 150 – Porta  $X$  quântica (CNOT quântica).

Fonte: (BRUMATTO, 2012)

Aplicando a porta  $X$  quântica a estados quânticos temos:

$$\begin{aligned}
 X|0\rangle &= |1\rangle & \text{e} & & X|1\rangle &= |0\rangle \\
 X(\alpha|0\rangle + \beta|1\rangle) &= \alpha X|0\rangle + \beta X|1\rangle \\
 &= \alpha|1\rangle + \beta|0\rangle \\
 X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}
 \end{aligned}$$

Figura 151 – Porta  $U$  unitária.

Fonte: (BRUMATTO, 2012)

### 10.11.3 Porta $U$ unitária

Aplicar uma porta sobre um *qubit* é o mesmo que utilizar uma matriz  $2 \times 2$ . Uma porta quântica deve ser *unitária*. Dada uma porta  $U$  qualquer, para que ela seja *unitária*, a seguinte relação deve ser válida, Figura 152:

$$U^\dagger U = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Figura 152 – Porta  $U$  unitária.

Fonte: (BRUMATTO, 2012)

Na equação acima,  $U^\dagger$  é o adjunto do operador  $U$ , ou seja, é o operador definido pela matriz transposta e conjugada. É fácil ver que  $X^\dagger X = I$ . O mais curioso é que só existe esta restrição para construção de portas quânticas.

Para o *qubit* podemos definir outras portas além da porta  $X$ .

Temos por exemplo, a Porta  $Z$ , que não altera o estado  $|0\rangle$ , mas muda o sinal do estado  $|1\rangle$  para  $-|1\rangle$ .

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Figura 153 – Porta  $Z$ .

Fonte: (BRUMATTO, 2012)

#### 10.11.4 Porta Hadamard

**Jacques Salomon Hadamard** (1865-1963) foi um matemático francês que contribuiu na teoria dos conjuntos, teoria das funções complexas, geometria diferencial, e equações diferenciais parciais. Por trabalhar com matriz, criou-se a uma porta quântica baseada em uma matriz apropriada.

A porta Hadamard  $H$  atua sobre 1 qubit e mapeia  $|0\rangle$  para  $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$  e mapeia  $|1\rangle$  para  $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ , que significa que uma medida em 1 *qubit* tem as probabilidades de ser 1 ou 0, o que representa a *sobreposição*).

A porta  $H$ , a porta de **Hadamard**, na Figura 155, ela é conhecida como "raiz quadrada de NOT".  $H$  é uma matriz unitária, já que  $H.H^* = \mathbb{I}$ , a matriz identidade.

A porta não é de fato a raiz quadrada de NOT, pois  $H^2 = I$ , ou seja, aplicar  $H$  duas vezes não irá alterar o estado de um *qubit*.  $H$  aplicada em  $|0\rangle$  transforma em  $(|0\rangle + |1\rangle)/\sqrt{2}$  e aplicada em  $|1\rangle$  transforma em  $(|0\rangle - |1\rangle)/2$ , ambos são estados que estão no meio do caminho de  $|0\rangle$  e  $|1\rangle$ . Por isso é chamada de raiz quadrada, ela faz uma *meia troca de bit*, podemos interpretar como um *deslocamento de fase*.

#### 10.11.5 As portas de Pauli

**Wolfgang Pauli** (1900-1958) é bem conhecido por seu trabalho em teoria do *spin* e a *teoria quântica*, bem como sua descoberta do *princípio de exclusão de Pauli* em 1925. Em 1931, ele previu a existência de *neutrinos*, partículas de interação fraca que viajam através do Universo quase à velocidade da luz.



Figura 154 – Jacques Hadamard - Teve uma de suas matrizes aplicada para definir uma porta quântica.

Fonte: <[https://pt.wikipedia.org/wiki/Jacques\\_Hadamard](https://pt.wikipedia.org/wiki/Jacques_Hadamard)>

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Figura 155 – Porta  $H$ : Hadamard.

Fonte: (BRUMATTO, 2012)

As portas  $X$  e  $Z$  são portas chamadas *Pauli-X* e *Pauli-Z*, na Figura 158, e estas compõem com a porta  $Y$  (*Pauli-Y*), as *portas de inversão*. As portas  $S$  (*Fase*) e  $T$  ( $\pi/8$ ) completam, com a porta  $H$ , as portas de *deslocamento de fase* e não podemos esquecer que os estados quânticos podem ser representados por números complexos. Podemos interpretar os índices de probabilidade na distribuição sobre os estados fundamentais como representação de fase na superfície de uma esfera de raio 1. As operações aplicadas através das portas quânticas são apenas operações de rotações nesta superfície, algumas portas indicam inversão (*flip*), e outras portas, rotações de um eixo para outro. Existem portas que oferecem uma rotação de fase menor que  $\pi/2$ . A porta de *Fase S* é considerada a raiz quadrada da porta  $Z$  de *Pauli* e a porta  $\pi/8$  é a raiz quadrada da *porta de Fase*, tal qual a porta **Hadamard** é a raiz quadrada da porta  $X$ .

Na realidade podem existir infinitas portas para um único *qubit*, no entanto, como

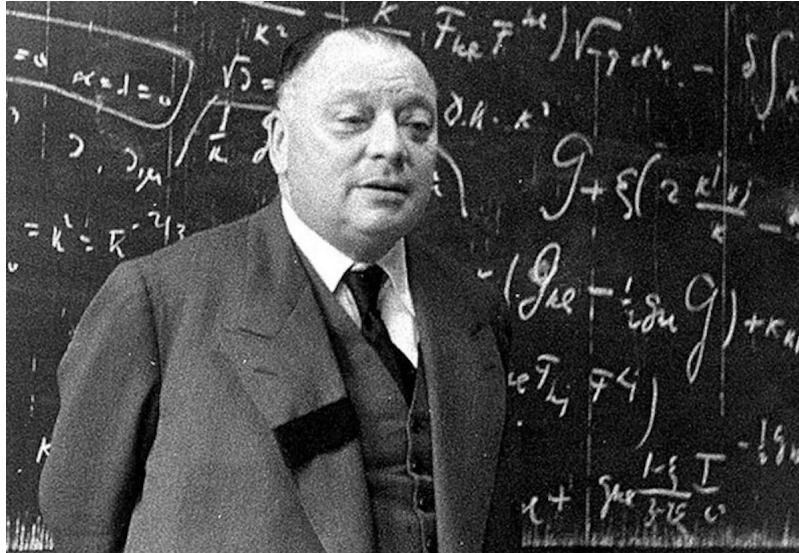


Figura 156 – Wolfgang Pauli - Teoria do Spin e o princípio de exclusão em 1925.

Fonte: Domínio público



Figura 157 – Portas de 2 bits da lógica clássica.

Fonte: (BRUMATTO, 2012)

as portas são *unitárias*, qualquer porta pode ser representada por um conjunto de rotações no campo dos números complexos.

## 10.12 Portas de $n$ qubits e Operações Quânticas

Se um sistema quântico possui múltiplos *qubits*, espera-se que as portas lógicas interajam com todos *qubits*, não apenas como operações isoladas em cada *bit*. Podemos fazer uma comparação com o modelo de dois *bits* clássicos, onde definimos um conjunto de portas que podem ser vista na Figura 157. Dentre estas, as portas NOT e (NOT AND) são consideradas universais, pois a partir destas duas é possível construir quaisquer outras portas. Algo semelhante se aplica à computação quântica. Na lógica clássica, uma porta AND possui duas entradas e fornece uma única saída.

$$\begin{aligned}
 \text{Pauli - Y} & : Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\
 \text{Fase} & : S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\
 \frac{\pi}{8} & : T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}
 \end{aligned}$$

Figura 158 – As portas Y (Pauli-Y) as portas de inversão. As portas S (Fase) e T ( $\pi/8$ ).

Fonte: (BRUMATTO, 2012)

Na lógica quântica, como os estados são representados por vetores de dimensão  $2^n$  ( $n$  é a quantidade de *qubits*) e os operadores são representados por matrizes de tamanho ( $2^n \times 2^n$ ) então a saída terá o mesmo número de entradas.

### 10.12.1 Porta CNOT quântica : NOT controlada

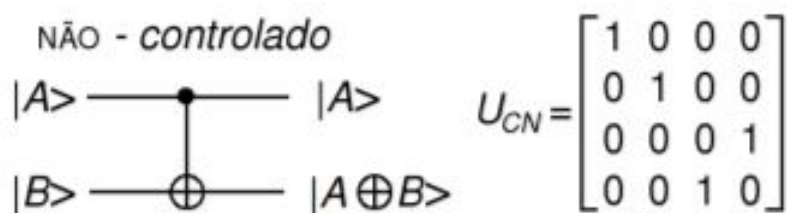


Figura 159 – Porta CNOT de 2 qubits da lógica quântica.

Fonte: Introdução à Computação Quântica (BRUMATTO, 2012)

A Figura 159 exibe a *porta NOT controlada* (CNOT) sobre dois *qubits*. A representação gráfica indica duas linhas de entrada representando cada *qubit*, a porta é representada como barra vertical com símbolos característicos nas extremidades, o círculo fechado representa o *bit* de controle da porta. Na mesma figura está a representação matricial da porta.

A porta CNOT atua realizando a operação da porta  $X$  no segundo *qubit*, somente se o primeiro (*qubit* de controle) estiver no estado  $|1\rangle$ , caso contrário não realiza qualquer alteração. Ou seja, a Tabela 160 abaixo indica entradas e saídas da porta CNOT.

A porta CNOT pode ser interpretada também através do uso da operação XOR (OR-eXclusive -  $\oplus$ ), como está representado na Figura 159  $U_{CN} |A, B\rangle \mapsto |A, A \oplus B\rangle$ , ou seja, a operação XOR entre o *qubit* de controle e o *qubit* alvo é armazenado no *qubit* alvo. Existem muitas outras portas para sistemas de 2 *qubits*, ou mesmo sistemas maiores, no entanto, a porta CNOT junto com portas de 1 *qubit* são protótipos para todas as outras portas, por causa do resultado notável sobre a universalidade das portas: *Qualquer porta lógica de múltiplos qubits pode ser construída a partir da*

$ 00\rangle$	$\mapsto$	$ 00\rangle$
$ 01\rangle$	$\mapsto$	$ 01\rangle$
$ 10\rangle$	$\mapsto$	$ 11\rangle$
$ 11\rangle$	$\mapsto$	$ 10\rangle$

Figura 160 – Tabela do operador CNOT aplicada aos estados fundamentais de um sistema de 2 qubits da lógica quântica.

Fonte: (BRUMATTO, 2012)

porta CNOT (NOT Controlada) e das portas de um qubit (NIELSEN; CHUANG, 2000).

Como exemplo, podemos ver na Figura 161 uma porta de TROCA que faz justamente a troca dos estados entre os dois *qubits*. As operações podem ser acompanhadas na equação abaixo:

$$\begin{aligned}
 |a, b\rangle &\mapsto |a, a \oplus b\rangle \\
 &\mapsto |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\
 &\mapsto |b, (a \oplus b) \oplus b\rangle = |b, a\rangle
 \end{aligned}$$

Figura 161 – Porta TROCA construída a partir de porta CNOT, que faz a troca dos estados entre os dois *qubits*.

Fonte: Introdução à Computação Quântica, Hamilton José Brumatto, UNICAMP.

A Figura 161 nos dá a ideia de um *circuito quântico*, o qual é representado por fios que indicam a passagem de cada *qubit* atravessando as portas quânticas. Existem algumas ações que não são permitidas nos circuitos quânticos, por exemplo a realimentação, permitida em circuitos lógicos clássicos, e diz-se que os circuitos quânticos são acíclicos.

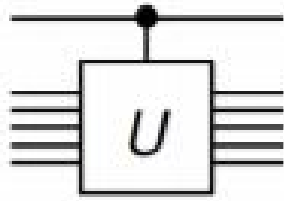
### 10.12.2 Porta U controlada para dois qubits

Portas para  $n$  *qubits* podem ser construídas conforme apresentado na Figura 162.

### 10.12.3 Medindo um qubit

Um último circuito importante, não que os demais sejam menos importantes, é o circuito para medir o *qubit*. Segundo os postulados da mecânica quântica (OMER, 2000), a medida  $M$  de um observável  $|\psi\rangle$  somente é determinística, se for um dos auto-estados (estado fundamental). Assim os comandos de teste não são mais resultados booleanos do sistema e sim, operações de medidas probabilísticas.

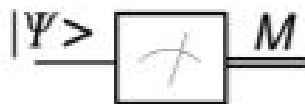
A medida do *qubit*, deve resultar, no entanto, o valor 0, ou 1, pois a medida de um estado quântico deve resultar um valor clássico. A Figura 163 indica um circuito onde os *qubits* são representados por linha simples, enquanto que os valores medidos para o sistema e indicados por bits clássicos são representados por linhas duplas.



### Porta *U*-Controlada para *n* Qubits

Figura 162 – Porta *U* controlada para 2 qubits.

Fonte: Introdução à Computação Quântica, Hamilton José Brumatto, UNICAMP.



### Circuito para medir o valor de um Qubit

Figura 163 – Circuito para medir o valor de um qubit.

Fonte: Introdução à Computação Quântica, Hamilton J. Brumatto, UNICAMP.

Devemos lembrar que a medida obtida do *qubit* que está no estado  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  tem probabilidade  $\alpha^2$  de ser o valor 0 e  $\beta^2$  de ser o valor 1, mas somente um valor será medido.

## 10.13 Computação reversível

O *princípio de Landauer* é um princípio físico relativo ao limite teórico mais baixo do consumo de energia da computação. Ele sustenta que "qualquer manipulação logicamente irreversível da informação, como o apagamento de um bit ou a fusão de duas trajetórias de computação, deve ser acompanhada por um aumento de entropia correspondente em graus de liberdade sem informação do dispositivo de processamento de informação (o processador) ou seu ambiente.

De acordo com o *Princípio de Landauer*, é possível construir um computador que dissipe uma quantidade de calor arbitrariamente pequena. Uma condição necessária para isso é que nenhuma informação seja perdida na computação. Desse ponto de vista, um outro modelo de computação torna-se necessário, tendo em mente que o atual, baseado em lógica irreversível, não atende a tal especificidade. Então, a lógica reversível tem papel fundamental neste novo modelo, observando que no limite teórico, um dispositivo construído sobre este alicerce não dissiparia calor. Neste trabalho, apresentamos a teoria da lógica reversível, mais especificamente, descrevemos as portas lógicas reversíveis, explorando o fato de que elas *formam*



um grupo simétrico e, assim, podemos empregar o ferramental da **teoria dos grupos**.

Então, é conveniente estarmos interessados em construir operações reversíveis no modelo clássico. Ao contrário de muitas portas lógicas clássicas, **as portas lógicas quânticas são reversíveis**. Para isso, precisaremos de mais duas portas para construir as funções desejadas. Denominaremos estas portas *FANOUT* e *EXCHANGE*. A primeira servirá para gerar dois "fios" com o mesmo pulso (ou bit) que o original. Já a segunda servirá para trocar os bits entre dois fios. A porta *NAND* não é reversível. Da mesma forma, outras portas, como *AND*, *OR*, *XOR* e outras, também não são. A única porta reversível é a *NOT*. Por exemplo, a porta quântica de **Toffoli** reversível pode implementar todas as funções booleanas aplicadas no caso clássico.

Como melhor prática da engenharia, queremos construir *circuitos reversíveis*, não será possível utilizar tais portas. Um exemplo de porta reversível é a porta *NOT*. Ao analisar a saída gerada por ela, sabemos qual foi o sinal recebido na entrada. Para construir o conjunto de portas necessárias para representar todas as funções de decisão, vamos utilizar, junto com a porta *NOT*, as portas *Controlled Not* (CNOT) e *Controlled Controlled Not* (CCNOT) (Toffoli gate, criada por **Tommaso Toffoli**). Estamos nos baseando nos estudos de **Charles Bennett** e **Gilles Brassard** ([BENNETT; BRASSARD, 1984](#)) sobre computadores reversíveis. A porta CNOT é um dispositivo com duas entradas  $A$  e  $B$  e duas saídas  $A_0$  e  $B_0$ . Podemos resumir o funcionamento dessa porta da seguinte maneira: o valor de  $A_0$  é sempre igual ao valor de  $A$ . Já o valor de  $B_0$  depende dos valores de  $A$  e de  $B$ . Se  $A = 1$ , então  $B_0$  vai ser a negação de  $B$ . Caso contrário,  $B_0 = B$ .

Analisando seu funcionamento, é fácil ver que esta porta é reversível. Além disso, podemos ver  $B_0$  como sendo a saída da função *xor* aplicada sobre as entradas  $A$  e  $B$ . A partir de uma porta CN, podemos construir também um circuito para a função *fanout* e um circuito para a função *exchange*. Como as quatro operações que temos, com as portas N e CN (*NOT*, *XOR*, *FANOUT* e *EXCHANGE*) não são suficientes para representar todas as funções, precisaremos de mais portas. Para que o conjunto fique completo, usaremos a porta CCN. O funcionamento da porta CCN é muito parecido com o da CN. Essa porta tem três entradas,  $A$ ,  $B$  e  $C$ , e três saídas,  $A_0$ ,  $B_0$  e  $C_0$ . Analogamente à porta CNOT, teremos  $A_0 = A$  e  $B_0 = B$ . Já o valor de  $C_0$  dependerá do valor de  $A$  e  $B$ . Se  $A = B = 1$ , então  $C_0$  terá o valor inverso de  $C$ . Caso contrário,  $C_0 = C$ . Esta porta é bastante poderosa. Se colocarmos sinal 1 na porta  $A$ , temos que  $B$ ,  $C$ ,  $B_0$  e  $C_0$  formam uma porta CN. Além disso, ao colocar sinal 0 em  $C$ , obtemos uma porta *AND*, tendo como entrada  $A$  e  $B$  e como saída  $C_0$ .

Neste ponto, temos as portas *AND*, *NOT*, *FANOUT* e *EXCHANGE*, que são suficientes para o que queremos. Logo, chegamos a um conjunto de portas que podem montar qualquer função de decisão desejada e que são todas reversíveis. Isso sugere que o poder computacional desses componentes não é inferior ao poder dos componentes usados para operações não-reversíveis.

## 10.14 Juntando as partes

Na seção anterior vimos uma introdução à construção de circuitos quânticos que permite dar os primeiros passos para a construção da arquitetura. Por exemplo, podemos ver na Figura 164 a construção de um circuito que realiza a "soma" de qubits.

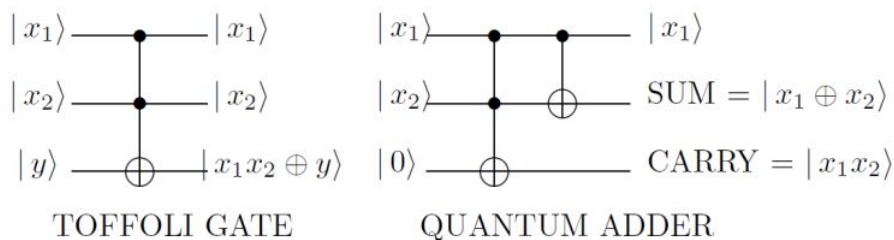


Figura 164 – Circuito de um somador quântico.

Fonte: Ekert, A., Hayden, P. M., and Inamori, H. Basic Concepts in Quantum Computation, vol. 72/2001 of Les Houches. Springer Berlin/Heidelberg, 2001.

Podemos imaginar, então, que a construção de um computador quântico é realizada integrando as diversas portas quânticas em uma rede quântica. No entanto várias complicações surgem [Isailovic \(2004\)](#). Primeiro, não existe o similar a um fio metálico que permita ligar as portas e carregar os *qubits*, muito pelo contrário, os *qubits*, no deslocamento, podem interagir com o ambiente alterando seu estado em um processo chamado *Descoerência*. Então é necessário um processo específico para transporte dos voláteis *qubits*.

De acordo com o teorema da **Não-Clonagem** ([ISAILOVIC, 2004](#)) é **impossível criar uma cópia exata de um *qubit* arbitrário**  $\alpha|0\rangle + \beta|1\rangle$ . O teorema da *Não-Clonagem* possui consequências severas no transporte quântico. Cada *qubit* precisa ser movido ponta-a-ponta e não copiado, desta forma é necessário construir *fios* confiáveis para este transporte. A ideia simplista de arremessar um *qubit* da origem ao destino é impraticável, pois o efeito de **Descoerência** pode ocorrer em vários momentos, na saída, ao longo do caminho e também na entrada, logo o *qubit* recebido não estará no estado inicial em que se pretendia transmitir.

Uma proposta ([ISAILOVIC, 2004](#)) mais viável é o uso da operação de troca, onde vários *qubits* alinhados operam a troca de forma que a informação de um *qubit* saia da origem e atinja o último *qubit*. O problema é que precisaríamos de uma rede de portas quânticas, e isto poderia aumentar o problema de *Descoerência*.

Um outro mecanismo importante é o *teleporte quântico*. Tanto a rede de troca, quanto o teleporte são viáveis no transporte da informação, mas ambos apresentam problemas, uma rede de troca não pode ser muito longa, pois o efeito da **Descoerência** acaba afetando o *qubit*, e isto impõe um limitante máximo para o caminho, e o teleporte implica em um mecanismo maior, inserido no caminho, o que limita o comprimento mínimo do caminho.

## 10.15 Teleporte Quântico

A Figura 165 apresenta um circuito que realiza o teleporte, onde é necessário um par EPR (Einstein-Podolsky-Rosen) para funcionar. O estado do *qubit* inicial que desejamos teleportar é  $|\Psi\rangle$ .

Vamos trabalhar com um sistema que utiliza o par EPR conhecido como:  $|\beta_{00}\rangle$ . O estado geral do sistema que envolve o *qubit* original e o par EPR  $|\Psi_0\rangle$  é:

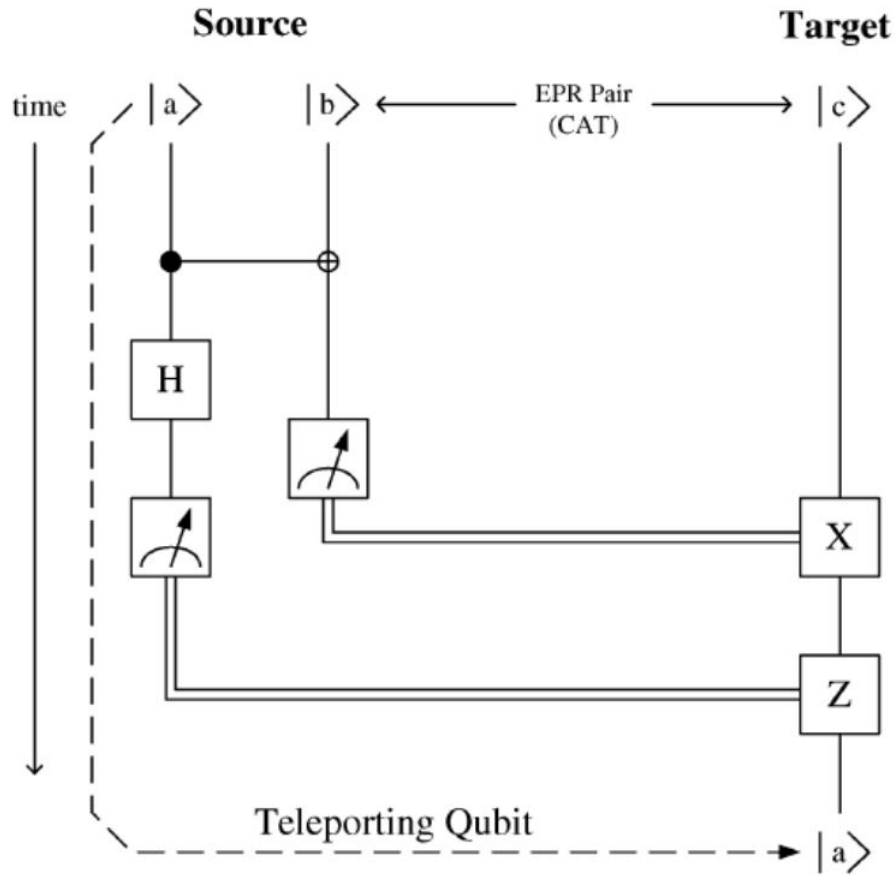


Figura 165 – Circuito quântico de teleporte (ISAILOVIC, 2004).

Fonte: Introdução à Computação Quântica, Hamilton José Brumatto, UNICAMP em (BRUMATTO, 2012).

$$|\Psi_0\rangle = |\Psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)] \quad (10.1)$$

O par EPR em um *Estado de Bell* é responsável pelo *teleporte*, o primeiro *qubit* está associado à origem e o segundo *qubit* do par está associado ao destino. Como vemos esta correlação na Figura 165 (ISAILOVIC, 2004). A equação acima na sua última linha apresenta o sistema inicial, associando o estado original do *qubit* a ser teleportado com o par EPR. Os dois primeiros *qubits* representam a origem, e o terceiro *qubit*, o destino. Ao aplicar CNOT com o *qubit*  $|\Psi\rangle$  como controle da porta NOT, atingimos o estado  $|\Psi_1\rangle$  para o conjunto:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)] \quad (10.2)$$

Observe que na probabilidade  $\beta^2$  do estado original ser 1, o primeiro bit do par EPR foi trocado através da porta NOT. Agora, aplicando-se a porta **Hadamard** sobre o bit original, ficamos com o estado  $|\Psi_2\rangle$ :

$$|\Psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \quad (10.3)$$

Após a medida dos dois *qubits* que descrevem o estado na origem representado na equação (10.9) (5.4) teremos somente o último *qubit* em um estado quântico:  $|\Psi_3\rangle$ , neste caso, seu estado é decorrente da correlação existente no par EPR, o estado  $|\Psi_3\rangle$ , será representado por apenas uma das quatro parcelas da soma acima. A Tabela 166 indica qual o estado final de  $|\Psi_3\rangle$  de acordo com o estado lido para os dois primeiros *qubits*. Para que o estado final do *qubit* no destino seja o estado do *qubit* original deve-se operar a troca de fase de acordo com os valores medidos: se o estado medido for  $|00\rangle$  então o estado de  $|\Psi_3\rangle$  já é uma cópia do estado original teleportado, se o estado medido for  $|01\rangle$  para atingir o estado original. É necessário fazer  $|\Psi_3\rangle$  passar por uma porta  $X$ , se for  $|10\rangle$  deve-se passar por uma porta  $Z$  e, se a medida indicar o estado  $|11\rangle$  deve-se passar pelas portas  $X$  e  $Z$  em sequência.

Alguns pontos interessantes no *teleporte*: é necessária uma medida clássica para que ele funcione, por outro lado a medida clássica impõe restrição na velocidade, não é possível teleportar um *qubit* em velocidades superiores à velocidade da luz, decorrente disto, não é possível teleportar uma informação para o passado (segundo os preceitos da teoria da relatividade) (NIELSEN; CHUANG, 2000). Outro fato é que o teleporte não é uma cópia do estado de um *qubit*, pois o *qubit* original se perdeu a partir do momento em que foi realizada a medida, restando somente o segundo *qubit* do par EPR original em um estado quântico idêntico ao estado do *qubit* original.

$$\begin{aligned} |00\rangle &\equiv \alpha|0\rangle + \beta|1\rangle \\ |01\rangle &\equiv \alpha|1\rangle + \beta|0\rangle \\ |10\rangle &\equiv \alpha|0\rangle - \beta|1\rangle \\ |11\rangle &\equiv \alpha|1\rangle - \beta|0\rangle \end{aligned}$$

**Tabela 2: Estado do Qubit teleportado após a realização da medida nos Qubits originais**

Figura 166 – Estado do qubit teleportado após a realização da medida nos qubits originais.

Fonte: Introdução à Computação Quântica, Hamilton José Brumatto, UNICAMP.

**Claude Crépeau** é membro do corpo docente da McGill University desde 1998. Ele foi um membro do Instituto Canadense de Pesquisa Avançada em Processamento de Informação Quântica de 2002 a 2012. Em 1993, juntamente com **Charles H. Bennett**, **Gilles Brassard**, **Richard Jozsa**, **Asher Peres** e **William Wootters**, criou o teleporte quântico.

## 10.16 Construindo a Arquitetura

Para construir uma arquitetura com base nas portas lógicas quânticas, enfrentamos para o transporte e armazenamento do *qubit* o problema da *Descoerência*,



Figura 167 – Teleporte quântico é de fato possível.

Fonte: (OLIVEIRA; PORTUGAL, 2008)

o estado de um *qubit* é volátil, e ele se perde principalmente por interação com o ambiente ou outra fonte de ruídos.

Para uma arquitetura viável é necessário *mecanismos de correção dos qubits* a fim de evitar resultados incorretos decorrente da *Descoerência*.

Esta tarefa apresenta duas dificuldades [Oskin, Chong e Chuang \(2002\)](#):

- A correção de um *qubit* difere de um bit clássico, pois o estado de um *qubit* é uma distribuição probabilística de um estado quântico, os erros ocorrem em um valor contínuo e não em um valor discreto como em bits clássicos, pequenas mudanças de fase já são fontes de erro.
- Outro motivo de dificuldade é o fato de que o estado deve ser corrigido sem que tenhamos conhecimento de qual é o estado, pois qualquer medida irá colapsar em um valor de estado fundamental.

Existe um mecanismo de correção eficiente ([OSKIN; CHONG; CHUANG, 2002](#)), utiliza-se um código  $[n; k]$ , onde  $n$  *qubits* são utilizados para codificar  $k$  *qubits* de dados. O circuito de correção de erro utiliza  $k$  *qubits* de dados e  $n - k$  *qubits* auxiliares. Estes são construídos a partir do estado  $|0\rangle$ . A decodificação verifica os  $n$  *qubits*,  $k$  são *qubits* de dados possivelmente errôneos, e  $n - k$  *qubits* que, com grande probabilidade, descreve o erro ocorrido. O circuito de correção, então aplica uma das  $2^{(n - k)}$  operações para corrigir o erro. O custo do mecanismo de correção de erro é a sobrecarga necessária para criar os estados codificados e executar os passos periódicos de correção de erro, na qual cada passo é uma operação tolerante a falhas ([OSKIN; CHONG; CHUANG, 2002](#)), que no entanto a eficiência é alta. Esta técnica aplicada recursivamente consegue que a taxa de erro caia exponencialmente com um custo polinomial do circuito de correção de erro.

Uma proposta de arquitetura de computador quântico pode ser vista na Figura [168](#), construída com base em caminhos de dados confiáveis e memória quântica eficiente. Podemos notar que a estrutura da arquitetura para computação quântica é

semelhante à clássica, no entanto alguns aspectos são únicos do domínio quântico. Como a Figura 168 mostra são definidos três componentes principais: a unidade lógica-aritmética quântica (qULA), a memória quântica e um escalonador dinâmico. É necessário usar a técnica de *teleporte* no transporte da informação quântica.

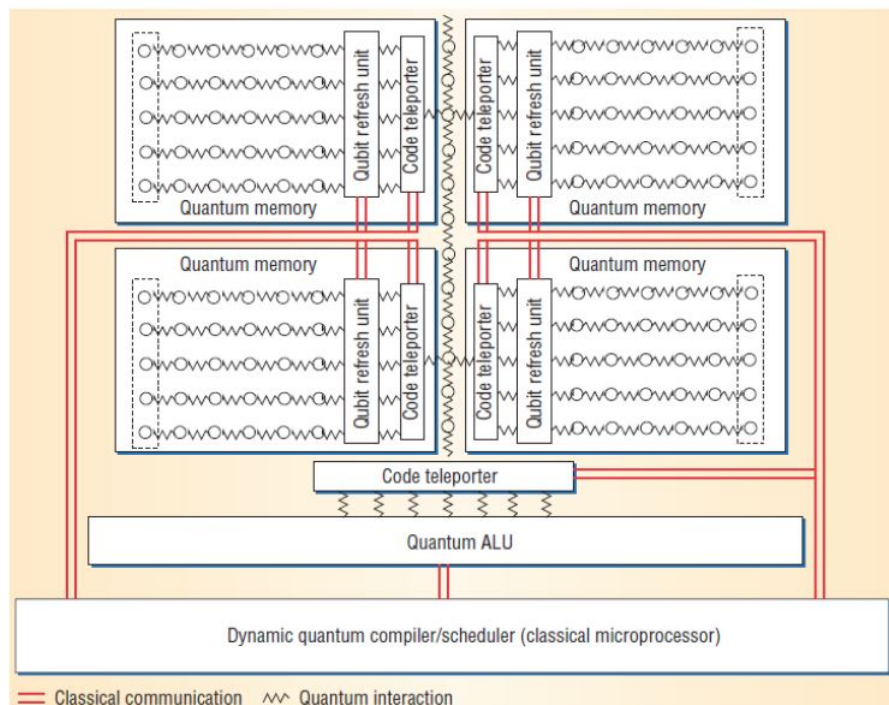


Figura 168 – Proposta de Arquitetura de Computador Quântico (OSKIN; CHONG; CHUANG, 2002).

Fonte: Introdução à Computação Quântica, Hamilton José Brumatto, UNICAMP.

Em eletrônica e circuitos digitais, o *flip-flop* ou multivibrador biestável é um circuito digital pulsado capaz de servir como uma memória de um bit. Um *flip-flop* tipicamente inclui zero, um ou dois sinais de *input*, um sinal de *clock*, e um sinal de *output*, apesar de muitos *flip-flops* comerciais proverem adicionalmente o complemento do sinal de *output*. Alguns *flip-flops* também incluem um sinal *clear*, que limpam a saída atual. A pulsação ou mudança no sinal do *clock* faz com que o *flip-flop* mude ou retenha seu sinal de saída, baseado nos valores dos sinais de entrada e na equação característica do *flip-flop*. O primeiro *flip-flop* eletrônico foi inventado em 1919 por **William Eccles** e **F. W. Jordan**. O nome posterior *flip-flop* descreve o som que é produzido em um alto-falante conectado a uma saída de um amplificador durante o processo de chaveamento do circuito. Precisar-se-á de algo similar a um *flip-flop* para se construir um *qubit*?

A construção de um mecanismo de memória confiável recai no uso de sistemas que oferecem uma taxa baixa de *descoerência* para *qubits* estáticos, mesmo assim, tal qual uma memória RAM, que "vaza" ao longo do tempo. O *qubit* armazenado ainda sofre com a *descoerência*, e esses dispositivos necessitam de unidades de *refresh*, que são menos complexas que uma qULA (Unidade Lógica e Aritmética quântica), mas também necessitam portas quânticas para gerar a correção de erros. O mecanismo de

*refresh* oferece a confiabilidade necessária para o conjunto de memória, no entanto, como são necessários muitos *qubits* para garantir a confiabilidade de um segundo, o mecanismo de correção de erro, são necessários vários módulos de memória. A qULA no núcleo da arquitetura executa as operações, tanto para computação, quanto para correção de erro. Ela é composta de um conjunto básico de portas quânticas:

- Hadamard
- Identidade (I, ou NOP quântico)
- Flip de Bit - O mesmo que a manipulação de bits que processa bits individuais - ( $\bar{X}$ , ou NOT quântico)
- Flip de Fase (Z)
- Flip de Bit e Fase (Y)
- Rotação por  $\pi/4$  (S)
- Rotação por  $\pi/8$  (T)
- NOT-controlada (C-NOT)

Estas portas formam o menor conjunto universal possível [Oskin, Chong e Chuang \(2002\)](#). As portas operam sobre dados codificados por correção de erro para garantir computação tolerante a falhas. Como são necessários os *qubits* auxiliares para a codificação e aplicação da correção de erro, um hardware específico deve gerar os *qubits* em estados elementares que serão utilizados pela qULA.

O transporte da informação é um desafio, como vimos, não é possível clonar um *qubit*, então optou-se por usar o mecanismo de *teleporte*, pois a rede de portas de troca acaba inserindo um ruído muito grande, comparado com o mecanismo de *teleporte*. O mecanismo de teleporte utiliza rede de portas de troca para transportar um dos bits do par EPR para o destino, para tanto não é necessário o uso de correção de erro, os bits do par EPR podem ser verificados facilmente por erro e independente do *qubit* físico a ser transmitido, ele pode ser descartado se houver erro e um novo par gerado. Uma vez o par correto, um *qubit* do par na origem e outro no destino, o bit físico pode ser teleportado através da distância desejada.

Esta arquitetura prevê um processador clássico de alta performance no controle de escalonamento dinâmico. Este usa construções clássicas de controle de fluxo e dinamicamente traduz as operações lógicas em operações sobre *qubits* físicos individuais. O algoritmo em execução utiliza o tamanho dos dados de entrada e as taxas de erros para os *qubits* físicos, para construir um controle de escalonamento dinâmico a fim de controlar a qULA, a unidade aritmética quântica, o teleporte de códigos e o *refresh* das unidades da qRAM (RAM baseada em *qubits*).

## 10.17 Computadores Quânticos podem funcionar

Existem quatro requisitos básicos para a implementação da computação quântica:

- Representação dos *qubits*.
- Operação das portas quânticas.
- Preparação dos estados iniciais.
- Medida do estado final dos qubits.

Algumas são as possibilidades abertas para construção de computadores quânticos, porém apenas duas representações fundamentais de *qubits* são utilizadas (NIELSEN; CHUANG, 2000): o *spin* e o *fóton*.

Existem quatro requisitos básicos para a implementação da computação quântica:

- Representação dos *qubits*;
- Evolução unitária controlável (operação das portas quânticas);
- Preparação dos estados iniciais (como para criar o par EPR);
- E a medida do estado final dos *qubits*.

Segue uma breve descrição de propostas de implementações que surgiram:

**Computador Quântico Ótico:** o qubit é representado pela localização de um único fóton em duas cavidades representadas pelos modos:  $|01\rangle$  e  $|10\rangle$ , ou mesmo pela sua polarização. As portas e transformações são construídas de deslocadores de fase, divisores de feixe e meios não-lineares que permite a modulação relativa de dois fótons. A dificuldade está na construção dos mecanismos não-lineares.

**Eletrodinâmica Quântica de Cavidades Óticas - EDQ:** baseado no acoplamento de um único átomo com alguns poucos modos óticos através do confinamento de átomos em cavidades com altos valores de  $Q$  (fator de qualidade). Nestas cavidades os átomos apresentam estados eletromagnéticos (fótons), e a representação dos *qubits* é dada pela localização de um único fóton entre dois modos. As portas são construídas da mesma forma que no Computador Ótico. A dificuldade também está no acoplamento de dois fótons, neste caso, mediado por um átomo.

**Armadilhas Iônicas:** uma das formas mais promissoras, os átomos aprisionados são resfriados até que sua energia cinética permita a distinção dos estados de *spin* do núcleo e do elétron. Os estados quânticos são representados pelos Spins:  $-3/2$ ,  $-1/2$ ,  $1/2$  e  $3/2$  que podem representar 2 qubits em seus quatro estados. As portas são construídas a partir de aplicações de pulsos de laser que manipulam os estados atômicos externamente. As dificuldades são: o tempo de *descoerência*, pois o tempo de vida dos fônons (estado de vibração dos *spins*) é muito curto, e preparar os íons no estado fundamental é uma tarefa difícil.

**Ressonância Magnética Nuclear:** A representação dos *qubits* se dá pelo *spin* de um núcleo atômico e sua precessão pela aplicação de campos magnéticos fortes. As portas são construídas pela aplicação de pulsos de campo magnético em um forte campo magnético estático. A dificuldade ocorre na preparação dos estados fundamentais e na leitura, o sinal de precessão é extremamente fraco.



Outras propostas - Outros esquemas são previstos, apesar da divulgação da empresa canadense *D-Wave Systems*<sup>3</sup> de já ter a construção do computador quântico com base em 128 *qubits*, a comunidade acadêmica se restringe a reconhecer propostas que evidenciam algumas naturezas quânticas principais, como *teleporte quântico* ou *estados EPR*. Os protótipos existentes definem computadores que chegam a alguns *qubits*. O quadro da Figura 169 mostra as perspectivas (com eram vistas até 2012) de futuro para a computação quântica. O progresso da pesquisa na computação quântica em direção ao computador quântico pode ser encontrado em **Quantum Computation Roadmap**.

QC Approach	The DiVincenzo Criteria							
	Quantum Computation						QC Networkability	
	#1	#2	#3	#4	#5		#6	#7
NMR								
Trapped Ion								
Neutral Atom								
Cavity QED								
Optical								
Solid State								
Superconducting								
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							

Legend:

- = Uma abordagem viável potencial atingiu prova suficiente do princípio
- = Uma abordagem viável potencial foi proposta, mas não há prova suficiente do princípio
- = Não é conhecida nenhuma abordagem
- #1 = Um sistema físico escalável com Qubits bem caracterizados
- #2 = Habilidade de iniciar Qubits em um estado simples garantido
- #3 = Tempo de descoerência longo, muito maior que o tempo de operação da porta
- #4 = Um conjunto universal de portas quânticas
- #5 = Capacidade de medir específicos Qubits
- #6 = Capacidade de trocar Qubits estacionários e em movimento
- #7 = Capacidade de transmitir de forma segura Qubits em movimento entre posições específicas

Figura 169 – Perspectivas da Computação Quântica (HUGHES R., 2010).

Fonte: <[http://qist.lanl.gov/qcomp\\_map.shtml](http://qist.lanl.gov/qcomp_map.shtml)>

**Quantum Computation Roadmap** - The overall purpose of this roadmap is to help facilitate the progress of quantum computation research towards the quantum computer science era. It is a living document that will be updated at least annually. Please e-mail comments on the quantum computation roadmap to **Richard Hughes** with a copy to **Malcolm Boshier**.

## 10.18 Computador quântico x Computador digital

Esta seção diz respeito a algumas considerações sobre o computador digital e o computador quântico.

<sup>3</sup> <http://www.dwavesys.com/>

- Já foi demonstrado que um computador digital pode ser simulado por um computador quântico. Logo, conclui-se que o computador quântico é ao menos tão poderoso quanto o computador digital.
- Considerando agora a possibilidade de simular um computador quântico empregando um computador digital, cabem as seguintes constatações:
- Um computador quântico com  $n$  *qubits* em superposição vai ter  $2^n$  autoestados.
- Isso implica que cada estado de um registrador quântico é definido por  $2^n$  números complexos.
- Cada operador quântico para este computador quântico de  $n$  *qubits* é descrito por uma matriz  $2^n \times 2^n$  de elementos complexos.
- A medida de cada *qubit* colapsa o estado em superposição resulta para um dos auto-estados, com certa probabilidade. O de maior probabilidade.

Portanto, para simular um *algoritmo quântico* em um computador digital, é necessário o seguinte:

- Memória suficiente para armazenar as  $2^n$  amplitudes complexas do registrador;
- Memória suficiente para armazenar as  $2^n \times 2^n$  amplitudes complexas de cada operador quântico;
- Dispor de operações básicas de álgebra matricial;
- Usar geradores pseudo-aleatórios para simular os resultados das medidas realizadas.
- Por que simular computadores quânticos em máquinas convencionais? Simulando computadores quânticos poderemos ter uma ideia das dificuldades a serem enfrentadas no desenvolvimento de novos algoritmos destinados a computadores quânticos. É interessante observar que antes do primeiro computador quântico ser construído, teremos diversos algoritmos específicos para computadores quânticos rodando em simulação. Além disso, através de simulações, teremos uma ideia muito aproximada do que poderemos esperar ao construir computadores quânticos.
- Em geral, vale a pena simular um sistema quando a simulação é imensamente menos custosa e ainda assim permite estudarmos os aspectos de interesse do sistema real. Esse é exatamente o motivo pelo qual trabalharemos com simuladores de máquinas quânticas.
- Além de uma demanda exponencial por memória, deve-se considerar a imprecisão numérica da representação em ponto flutuante para valores reais e a imprecisão estatística ao empregar-se geradores de números pseudo-aleatórios na computação digital.
- Como um exemplo, supondo que um número real possa ser representado aproximadamente por 4 bytes em um computador digital, são necessários 8 Gigabytes para representar um estado arbitrário de 30 *qubits* em superposição:  $2 \times 2^{30}$  valores em ponto flutuante para as partes real e imaginária dos números complexos, cada qual requerendo 4 bytes.

## 10.19 O computador e a computação quântica

Na mecânica quântica é possível que uma partícula esteja em dois ou mais estados ao mesmo tempo. Um computador clássico tem uma memória feita de bits. Cada bit guarda um "1" ou um "0" de informação. Mas, um computador quântico mantém um conjunto de *qubits*. Um *qubit* pode conter um "1", um "0" ou uma sobreposição destes. Em outras palavras, pode conter tanto um "1" como um "0" ao mesmo tempo. O computador quântico funciona pela manipulação desses *qubits*. Um exemplo desse fato é o gato de **Schrödinger**. Imagine que um gato esteja dentro de uma caixa, com 50% de chances de estar vivo e 50% de chances de estar morto; para a mecânica quântica, até abrirmos a caixa e verificarmos como está o gato, ele deve ser considerado vivo e morto ao mesmo tempo. A esta capacidade de estar simultaneamente vivo ou morto, chama-se **sobreposição/superposição**. Mas, depois de aberta a caixa, um dos dois estados do gato deixa de existir (colapsa) para um destes estados e prevalece o outro: vivo ou morto.

Um computador quântico é um dispositivo que executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como *sobreposição* e *entrelaçamento/emaranhamento/interferência*.

A teoria da mecânica quântica, um dos pilares da Física do século XX, nos ensina que **a estrutura fina da matéria é mais sutil** do que nos parece. Um **computador quântico** pode ser construído com alguns sistemas com **partículas** muito pequenas, **desde que obedeçam à natureza da matéria, descrita pela mecânica quântica**. Pode-se construir computadores quânticos com **átomos que podem estar excitados e não excitados ao mesmo tempo**, ou com **fótons que podem estar em dois lugares ao mesmo tempo**, ou com **prótons e nêutrons**, ou ainda com **elétrons e pósitrons que podem ter estados de *spin* ao mesmo tempo "para cima" e "para baixo"** e se **movimentam em velocidades próximas à da luz**. Com a utilização destes tipos de partículas da matéria, ao invés de nano-cristais de silício, **o computador quântico tem o poder de processamento, exponencialmente muito mais rápido**.

Uma molécula microscópica pode conter muitos prótons e nêutrons, e pode ser usada como computador quântico com muitos *qubits*. Cada um desses *qubits* pode representar 0 ou 1 (como um bit convencional), mas também os dois valores ao mesmo tempo, a chamada "sobreposição de estados". É essa capacidade que **umenta exponencialmente as velocidades computacionais** num computador quântico. Normalmente, a computação em um computador quântico termina com uma medição. Isso leva a um *colapso do estado quântico a um dos estados-base*. Pode ser dito que o estado quântico é medido para estar no estado correto com uma probabilidade alta.

É neste ponto que residem os problemas. A maioria dos **erros** acontece quando um *qubit* está nos dois estados: eles podem voltar a ser apenas um 0 ou 1 (um destes estados quânticos deixa de existir (o estado é colapsado), prevalecendo o de maior probabilidade, e desacelerando a computação).

Em computação quântica, um *algoritmo quântico* é um algoritmo que funciona em um modelo realístico de computação quântica. ([GERSHENFELD; CHUANG, 1998](#)) ([MOSCA, 2008](#)). O modelo mais utilizado é o modelo do circuito de computação quântica ([KITAEV, 1997](#)). A terminologia em geral se refere àqueles algoritmos que

utilizam das propriedades da computação quântica, como a sobreposição quântica ou entrelaçamento quântico. Exemplos de algoritmos quânticos estão em (MOSCA, 2008).

## 10.20 Simulação de sistemas quânticos

Aqui estão alguns links que foram encontrados na Internet, no sentido de podermos executar algum programa quântico. Provavelmente, cada um desses ambientes, deve proporcionar os meios de submeter um programa-exemplo. Entretanto, os autores ressaltam que estudos sobre algoritmos quânticos e sobre linguagens de programação quântica serão disponibilizados em volume separados na **Série Pensamento Matemático @ Ciência da Computação**. Um trabalho interessante sobre simulação de circuitos quânticos está em (CABRAL; JR; LIMA, 2005) (Zeno Simulator).

Alguns simuladores quânticos:

- (1) Estados Quânticos Ligados - Partículas Quânticas, Poço de Potencial - Em <[https://phet.colorado.edu/pt\\_BR/simulation/bound-states](https://phet.colorado.edu/pt_BR/simulation/bound-states)>
- (2) Simulação da transformada quântica de fourier com o simulador Zeno - Em <<https://periodicos.ufersa.edu.br/index.php/ecop/article/view/7894/6975>>
- (3) Simulando Algoritmos Quânticos em um Computador Clássico - Em <<https://app.uff.br/riuff/bitstream/1/5730/1/monografia.pdf>>
- (4) Experimente o "computador quântico em nuvem" da Google (tente procurar).
- (5) O Computador Quântico da IBM e o IBM Quantum Experience - Em <[www.scielo.br/pdf/rbef/v39n1/1806-1117-rbef-39-01-e1301.pdf](http://www.scielo.br/pdf/rbef/v39n1/1806-1117-rbef-39-01-e1301.pdf)>
- (6) OpenSimulator is an open source multi-platform, multi-user 3D application server - Em <[http://opensimulator.org/wiki/Main\\_Page](http://opensimulator.org/wiki/Main_Page)>
- (7) A High Performance Quantum Computer Simulator (Using OpenCL and Python) - Em <<https://qcgpu.github.io/>>

## 10.21 Dois tipos de computadores quânticos

A Figura 170 mostra dois tipos de computadores quânticos sendo atualmente em pesquisa, imaginando-se aplicações, generalidade e poder computacional. O caso *analógico* é o que está mais próximo, e que já existem máquinas construídas.

## 10.22 Computadores quânticos - outros marcos importantes

- 1993 - **Charles Henry Bennett** (1943) (IBM): um físico, criptógrafo e cientista da computação estadunidense. É um dos descobridores do *teletransporte quântico* <[https://pt.wikipedia.org/wiki/Charles\\_Henry\\_Bennett](https://pt.wikipedia.org/wiki/Charles_Henry_Bennett)>. Charles

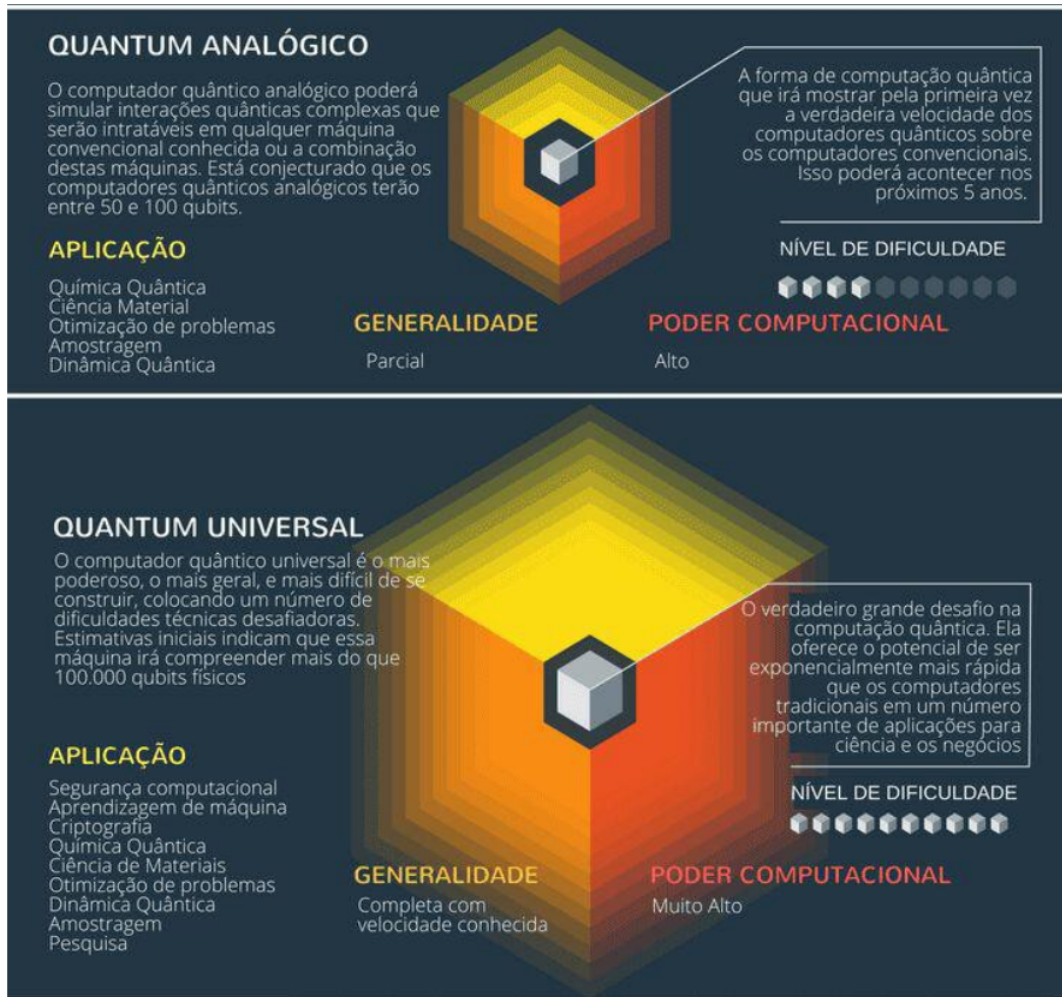


Figura 170 – Dois tipos de computadores quânticos - Aplicações, generalidade e poder computacional.

Fonte: <<https://www.cryptoradar.com.br/tecnologia/a-computacao-quantica-pode-destruir-as-criptomoedas/>>

<<https://www.cryptoradar.com.br/tecnologia/a-computacao-quantica-pode-destruir-as-criptomoedas/>>

Bennett e colaboradores da IBM mostram que a teleportação é de fato possível, desde que se destrua a amostra original.

- 1994 - **Peter Shor**, no Bell Labs da AT&T em Nova Jersey, descobriu um excelente algoritmo. Esse algoritmo permite a um computador quântico fatorar grandes inteiros rapidamente. Ele resolve tanto o *problema da fatoração* quanto o *problema do logaritmo discreto*. O algoritmo de **Shor** poderia, em teoria, quebrar muitos dos sistemas criptográficos em uso atualmente. Essa descoberta criou um enorme interesse nos computadores quânticos, até mesmo fora da comunidade acadêmica <[https://pt.wikipedia.org/wiki/Algoritmo\\_de\\_Shor](https://pt.wikipedia.org/wiki/Algoritmo_de_Shor)>.
- 1996 - **Lov K. Grover** (1961) - É um cientista informático indiano. Ele é o originador do algoritmo de busca de base de dados, usado na computação quântica. Ele é o inventor do que foi provado ser o mais rápido possível algoritmo de busca que pode ser executado em um computador quântico. A proposta é a de um algoritmo quântico para busca em uma base de dados, quadraticamente

mais rápido que os análogos clássicos. É também proposto o primeiro esquema para correção de erro quântico. Isso é uma aproximação a computadores quânticos que podem processar grandes números de *qubits* por longos períodos de tempo. Erros sempre são introduzidos, mas uma forma de correção de erros quânticos pode sobrescrevê-los e corrigi-los. Esta pode ser a chave tecnológica para a produção em larga escala de computadores quânticos que realmente funcionam. Estas propostas adiantadas tiveram um certo número de limitações. Poderiam corrigir alguns erros, mas não erros que ocorrem durante o próprio processo da correção. Algumas melhorias foram sugeridas, e a pesquisa sobre este tema continua ativa (GROVER, 1996) (GROVER, 1999) (GROVER, 2001).

- 1998 - **Isaac L. Chuang** (1968) recebeu os graus de graduação em física e engenharia elétrica e mestrado em engenharia elétrica no MIT. Em 1997, ele recebeu seu PhD em engenharia elétrica da Universidade de Stanford, e em 1998 desenvolveu o primeiro computador quântico de 1 qubit. **Chuang** lidera um grupo de pesquisa no *Massachusetts Institute of Technology*.

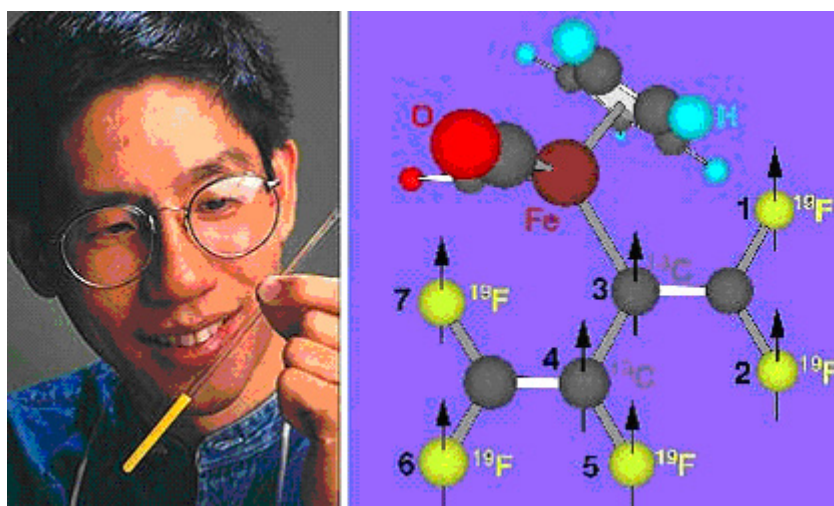


Figura 171 – Isaac Chuang segura frasco com solução com as moléculas que funcionaram como um computador quântico; à dir., estrutura da molécula. As operações que permitiram fatorar o número 15 foram realizadas pelos átomos numerados de 1 a 7.

Fonte: <<https://student.dei.uc.pt/~rsalgado/AC2/#links>>

- 1999 - No MIT foram construídos os primeiros computadores quânticos baseados em montagem térmica. O computador é, na verdade, uma única molécula pequena, que armazena *qubits* na rotação (*spin*) de seus prótons e nêutrons. Trilhões e trilhões destas moléculas podem flutuar em um copo da água. O copo está colocado em um equipamento de ressonância magnética nuclear, similar à imagem por ressonância magnética das máquinas usadas em hospitais. *Quantum Computing with Molecules* pode ser entendida em (GERSHENFELD; CHUANG, 1998).
- 2001 - IBM: computador quântico de 7 qubits que fatora o número 15 usando o algoritmo de **Peter Shor**. Em 1994, o cientista **Peter Shor** desenvolveu um método teórico para que computadores quânticos conseguissem fatorar um

número, ou seja, encontrar os números primos que, multiplicados, resultem no número inicial. O método, que ficou conhecido como algoritmo de Shor, previa a utilização das propriedades quânticas dos átomos para agilizar operações semelhantes às realizadas em computadores comuns, em que os dados são processados por chips de silício.

- 2007 - Empresa canadense D-Wave afirmou ter desenvolvido um computador híbrido chamado Orion que inclui um processador quântico de 16 qubits mas que também processa bits convencionais <<http://www.dwavesys.com/>>.
- 2016 - Computador quântico da IBM agora está disponível para uso público: a *IBM Quantum Experience* com 16 qubits: <<https://quantumexperience.ng.bluemix.net/qx/editor>>.
- 2017 - A D-Wave Systems lançou comercialmente o 2000Q, um computador quântico de 2000 qubits a módicos US\$ 15 milhões. O computador quântico anterior da companhia tinha 1.000 qubits. Esses sistemas estão sendo testados pelo Google, NASA e pela Lockheed Martin.

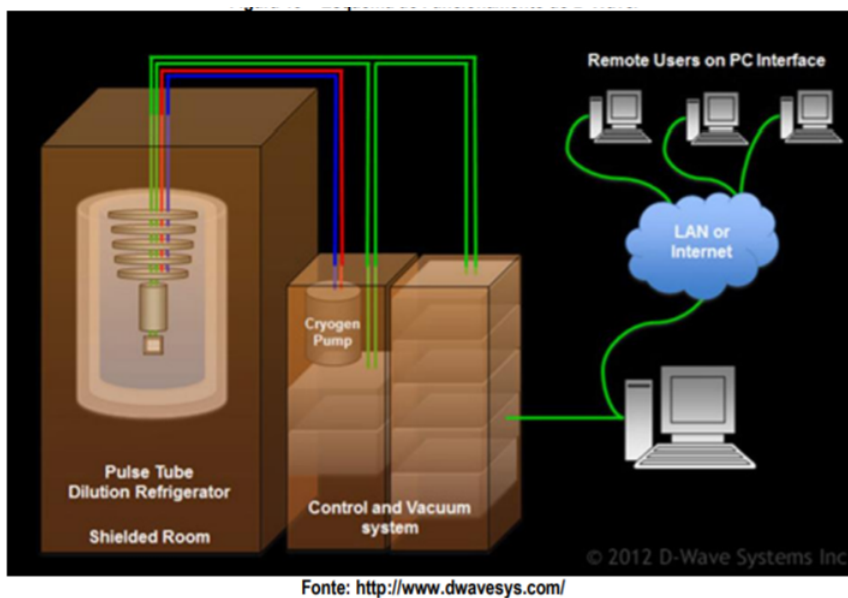


Figura 172 – Esquema de funcionamento do D-Wave-2.

Fonte: <[revista.unilus.edu.br/index.php/ruep/article/download/745/u2016v13n31e745](http://revista.unilus.edu.br/index.php/ruep/article/download/745/u2016v13n31e745)>

- 2017 - O físico brasileiro **Guilherme Tosi**, juntamente com uma equipe de pesquisadores da Universidade de Nova Gales do Sul, na Austrália, inventou uma nova arquitetura radical para a computação quântica, baseada em 'flip-flop qubits' que pode ser usada em um novo tipo de computador quântico permitindo, assim, a fabricação de processadores quânticos em larga escala, sem a necessidade do processo complicado da colocação precisa dos átomos de silício no processador <<https://engenheironaweb.com/2017/09/12/brasileiro-cria-nova-arquitetura-de-computacao-quantica-inovadora/>>.
- 2019 - *Q System One* é o computador quântico da IBM DE 17 qubits criado para empresas.

- 2019 - *IonQ* é o computador quântico da IonQ, de 79 qubits construído com itérbio.

## 10.23 Conheça o IonQ

O *IonQ* é o último computador quântico de que se noticiou em 04 de Janeiro de 2019. Com 79 *qubits*, o dispositivo superou o *Bristlecone*, antigo recordista do **Google**. Além das especificações superiores, o *IonQ* também bateu todos os outros computadores quânticos, no cálculo de solução de problemas matemáticos, que é usado para definir o potencial desse tipo de máquinas. Em vez do *silício super resfriado* a temperaturas próximas do zero absoluto, usa *íons do metal itérbio suspenso em um campo eletromagnético*, em uma abordagem batizada pelos criadores de "*trapped ion*" (ou "íon capturado", em tradução direta). Nesse campo eletromagnético, em que o itérbio fica aprisionado, engenheiros manipulam lasers que leem, armazenam e enviam informações ao computador.

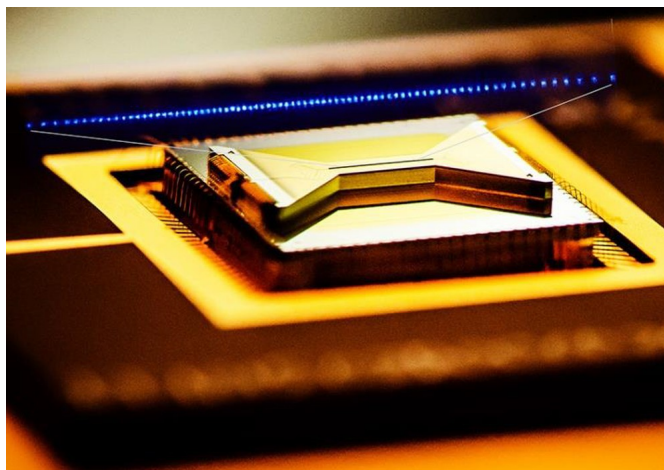


Figura 173 – Ionq-chip - O IonQ funciona com a captura de íons de itérbio num campo eletromagnético.

Fonte: Foto: Divulgação/IonQ

Uma característica do *IonQ* que ganha destaque é sua alta precisão. A máquina chega a 99.97% de precisão para um único qubit, enquanto o recordista anterior chegava a 99.5%, e 99.3% para o uso de dois qubits, valor máximo até então de 95%.

O itérbio é um elemento químico da tabela periódica que apresenta símbolo *Y* e número atômico 70 (70 prótons e 70 elétrons) com massa atômica 173 u.m.a (u). O itérbio é um elemento metálico prateado e macio. É uma terra rara da série dos lantanídeos que é encontrado nos minerais gadolinita, monazita e xenótimo.

A empresa IonQ aposta no conceito de íons capturados como o futuro dos computadores quânticos, mas reconhece que sua solução inovadora também tem seus problemas. O projeto acaba forçando a criação de máquinas fisicamente muito maiores e a velocidade por operação ainda não é competitiva frente a outras apostas. Apesar disso, destaca que essa tecnologia é altamente escalável, permitindo implementações com muito mais *qubits* sem grandes modificações.



## 10.24 História, Startups e Perspectivas

A chamada Lei de **Moore** (Gordon Moore - 1965) previu o número de átomos necessários para representar um bit de informação nos computadores atuais, alcançaria a escala atômica (NIELSEN; CHUANG, 2002). Nestas dimensões a descrição dos fenômenos físicos deve ser feita através da mecânica quântica. A Computação Quântica (CQ), que baseada na *estrutura fina da matéria*, surgiu no início da década de 80, é uma das alternativas tecnológicas mais importantes, pois seu desenvolvimento permitirá a criação de computadores extremamente rápidos, que realizarão em minutos cálculos que levariam centenas de anos, e redes seguras de computadores, com o surgimento da criptografia quântica (MACHADO, 2008).

O grande interesse da comunidade científica em *computação quântica*, e também em *informação quântica*, se deve-se à larga gama de possíveis aplicações e desenvolvimentos, em várias áreas, como: matemática, física, química, entre outras áreas. Ainda nos seus primórdios - pode-se comparar à época em que os transistores foram descobertos- a computação quântica surge como uma alternativa tecnológica com diversas vantagens sobre a computação clássica. Utilizando os conceitos desenvolvidos na área, alguns *algoritmos quânticos* foram criados, como os apresentados neste capítulo, e apresentaram um surpreendente desempenho, sendo muito mais rápidos do que seus análogos clássicos.

Outro desenvolvimento derivado da **computação quântica** é a **criptografia quântica**, já utilizada em redes criadas, que impossibilita a ação de "*hackers*" e possibilita a distribuição segura de chaves públicas. Ao mesmo tempo, sistemas magnéticos de dimensões reduzidas ou na forma de filmes finos ou de sistemas nano-estruturados têm apresentado um amplo espectro de fenômenos interessantes nas últimas décadas, entre eles a utilização das propriedades magnéticas dos elétrons - o *spin* - para realizar operações lógicas quânticas. O crescente interesse em Computação Quântica (CQ) é devido principalmente a dois fatores: (a) a descoberta desses algoritmos quânticos ultra-rápidos, capazes de realizar em minutos ou horas tarefas que levariam bilhões de anos em computadores clássicos; (b) o desenvolvimento de novas técnicas experimentais e sistemas que permitiram a demonstração experimental destes algoritmos.

A partir de 1997, a história fantástica da computação quântica continua até os dias de hoje, e o leitor pode ver parte desta história na introdução em (MACHADO, 2008), além de história e conceitos em (FALCAO; MOLINARI, 2016) e (ALVES, 2003). Existem os projetos de computação quântica das grandes corporações de tecnologia como (IBM, Google, Microsoft, Intel). Além desses, ver **D-Waves Systems** em <<https://www.dwavesys.com/home>>.

Existem diversas *start-ups* no ramo quântico, tais como **IonQ** em <<https://ionq.co>> e <<https://en.wikipedia.org/wiki/IonQ>>; a **Rigetti Computing** <<https://www.rigetti.com/>>, uma desenvolvedora baseada em Berkeley, na Califórnia, de circuitos integrados quânticos usados em computadores quânticos. A empresa também desenvolve uma plataforma de nuvem chamada *Forest* que permite que os programadores escrevam algoritmos quânticos; **1QBit Information Technologies** é uma empresa de software de computação quântica, com sede em Vancouver, British Columbia. A **1QBit** <<http://www.1qbit.com/>> (2012) e estabeleceu parcerias de hardware com a Microsoft, IBM, Fujitsu e D-Wave Systems; a **qci** em

<<https://quantumcircuits.com>>; a **CQC (Cambridge Quantum Computing)** é uma empresa de computação quântica independente, com sede em Cambridge, Inglaterra. Fundado em 2014, o **CQC** cria ferramentas para a comercialização de tecnologias quânticas com foco em software quântico e segurança cibernética quântica; a **QxBranch** (2014) <<http://www.qxbranch.com/>> é uma empresa de software de análise de dados e computação quântica, com sede em Washington, DC. A empresa fornece serviços de análise de dados e pesquisa e desenvolvimento para a tecnologia de computação quântica; a **QC Ware** em <<https://qcware.com/>>; a Starngeworks (2017) em <<https://strangeworks.com/>>; a **Quintessence Labs Pty Ltd.** <<https://www.quintessencelabs.com/>> é uma empresa de segurança cibernética sediada em Canberra, Austrália, com escritórios em San Jose, Califórnia, em ; a **Zapata Computing** em <<http://zapatacomputing.com/>>; a **artist.qb** em <<https://artiste-qb.net>>; a **Horizon** <<http://horizonquantum.com/>>; a **Quantum Benchmark** em <<http://quantumbenchmark.com/>> e a IDQ (ID Quantique) em <<http://www.idquantique.com/>>. Uma lista completa de empresas no ramo quântico, contendo estas *startups* já mencionadas, está em <<https://quantumcomputingreport.com/players/privatestartup/>>.

Existem também a **QISKit** em <<https://www.qiskit.org/>> e a **ProjectQ** em <<https://projectq.ch/>>, Embora não sejam *startups*, também merecem uma menção como importantes projetos de software quântico.

## 10.25 Bibliografia e Fonte de Consulta

Centro de Computação Quântica, Universidade de Oxford - <<http://www.qubit.org>>

Computador Quântico - <[https://pt.wikipedia.org/wiki/Computador\\_quântico](https://pt.wikipedia.org/wiki/Computador_quântico)>

<https://pt.wikipedia.org/wiki/NP-completo>

<https://pt.wikipedia.org/wiki/BQP>

QUARESMA, Pedro. Computabilidade e Complexidade, Departamento de Matemática, Universidade de Coimbra, Portugal, 2012.

Gershenfeld, Neil; Chuang, Isaac L. (junho de 1998). Quantum Computing with Molecules (PDF-<http://cba.mit.edu/docs/papers/98.06.sciqc.pdf>). Scientific American.

Mosca, M. (2008). Quantum Algorithms. quant-ph. arXiv:0808.0369, acessível livremente em (<https://arxiv.org/abs/0808.0369>).

Kitaev, A. Yu. (1997), Quantum computations: algorithms and error correction, Uspekhi Mat. Nauk (em russo), 52 (6(318)): 53-112,

Montanaro, Ashley (12 de janeiro de 2016). Quantum algorithms: an overview. npj Quantum Information (em inglês). 2. 15023 páginas. doi:10.1038/npjqi.2015.23

Circuito Quântico - <[https://pt.wikipedia.org/wiki/Circuito\\_Quântico](https://pt.wikipedia.org/wiki/Circuito_Quântico)>

Circuitos Quânticos -

<<http://ppginf.ucpel.tche.br/weciq/CD/Mini-Cursos/BernardoLulaJr/mini-curso-bernardo-lula>>

[pdf](#)>

Histórico, Estado e Perspectivas da Tecnologia da Computação QuânticaBQ - RUEP  
<[revista.unilus.edu.br/index.php/ruep/article/download/745/u2016v13n31e745](http://revista.unilus.edu.br/index.php/ruep/article/download/745/u2016v13n31e745)>

## 10.26 Para saber mais ... Leitura Recomendada

Daniel I. A. Cohen. Introduction to Computer Theory. Wiley and Sons, Inc. New York. Second Edition, 1997.

Marc Davio et al. Discrete and Switching Functions. Georgi Publishing Co. & McGraw-Hill, 1978.

J. E. Hopcroft. Introduction to Automata Theory Languages, and Computation, Addison-Wesley, 1979.

Zvi Kohavi. Switching and Finite Automata Theory, McGraw-Hill, 1978.

J. van Leeuwen. Handbook of Theoretical Computer Science, MIT Press, 1990.

H. R. Lewis, C. H. Papadimitriou. Elements of the Theory of Computation (2nd Edition), Prentice-Hall, 1996.

# Algoritmos e Computação Quântica

Qualquer pessoa que tenha algum conhecimento sobre computação, sabe que para um computador desenvolver determinada tarefa é necessário programá-lo. E antes disso, é imprescindível elaborar um bom algoritmo, que por sua vez, são implementados transformando-se em programas de computador. Contudo, com o advento da computação quântica, programas convencionais ficarão obsoletos. Ou melhor, não somente esses programas, mas a teoria utilizada para elaborá-los ficará obsoleta. Dessa forma, quando essa nova revolução ocorrer, os programas deverão ser construídos a partir de *algoritmos quânticos*. É justamente neste ponto que aparece um novo desafio, pois com esse novo paradigma, os futuros programadores deverão conhecer bem a forma como a informação deve ser tratada na perspectiva quântica, de forma que deter conhecimento sobre mecânica quântica deixará de ser um privilégio restrito aos físicos.

## 11.1 Um Algoritmo Quântico em geral

- Um algoritmo quântico, em sua estrutura básica, é composto por:
  1. Especificação de  $n$  *qubits*;
  2. Aplicação sequencial de  $k$  operadores quânticos sobre quaisquer subconjuntos dos  $n$  *qubits*;
  3. Medição realizada sobre qualquer subconjunto de *qubits*.
- Logo, o resultado só pode ser auferido *probabilisticamente*.
- Múltiplas execuções do mesmo algoritmo (redundância) e estratégias de projeto podem fazer com que a solução se aproxime de um resultado *determinístico*.

Um trabalho importante é a tese de doutorado em ([KOWADA, 2006](#)) que aborda a construção de algoritmos reversíveis e quânticos.

Existem alguns algoritmos quânticos propostos, que de certa forma apresentam

considerável vantagem sobre os algoritmos clássicos. O primeiro deles, o algoritmo de **Deutsch-Jozsa** é um algoritmo quântico, proposto por David Deutsch e **Richard Jozsa** in 1992 [1], e melhorado por **Richard Cleve**, **Artur Ekert**, **Chiara Macchiavello** e **Michele Mosca** em 1998 [2]. Apesar de possuir uma aplicação prática limitada, trata-se de um dos primeiros exemplos de um algoritmo quântico. O segundo, o algoritmo de **Peter Shor** (1994). E o terceiro, aqui apresentado é o algoritmo de **Grover** (1996). Mas, devido aos problemas de colocação de figuras do LaTeX, este texto mostra: (1) **Shor**; (2) **Grover**; (3) **Deutsch-Jozsa**.

## 11.2 Preparando para entender o algoritmo de Shor - 1994

Um segundo algoritmo quântico foi desenvolvido por **Peter Shor** em 1994 que será mais detalhado na seção 11.2.1. Na teoria da complexidade computacional e em computação quântica, o algoritmo de **Shor** é um algoritmo quântico, para fatorar um número  $N$  não primo de  $L$  bits.

Usando bits quânticos, ou *qubits* reciclados, o cálculo quântico de **Shor** é utilizado, explorando a mecânica quântica, para simplificar a fatoração de números em seus componentes principais - uma tarefa difícil para os computadores comuns, quando os números ficam muito grande. Até 2012, o maior número fatorado usando o algoritmo de **Shor** era 15.

### 11.2.1 Algoritmo de Fatoração de Shor

**Peter Williston Shor** (1959) é um matemático estadunidense. É professor do Departamento de Matemática, na área de matemática aplicada no Instituto de Tecnologia de Massachusetts (MIT). É conhecido por seu trabalho em **computação quântica**, em particular pela elaboração do algoritmo de Shor, um algoritmo quântico para fatorar exponencialmente mais rápido que o melhor algoritmo conhecido atualmente rodando em um computador clássico. O trabalho de **Shor**, equivale nos tempos de hoje, ao trabalho de **Turing** que, na década de 30, pensava em computação sem computador. **Shor** pensou em computação quântica sem ter um computador quântico.

Com um computador digital crê-se ser capaz de simular qualquer dispositivo de computação física com um aumento no tempo de cálculo de um fator de, no máximo, *polinomial*. Isso não pode ser verdade quando a mecânica quântica é levado em consideração. O trabalho de **Peter Shor** em (<http://arxiv.org/abs/quant-ph/9508027>) considera **fatorar inteiros** e **encontrar logaritmos discretos**, dois problemas que são geralmente difíceis em um computador clássico e têm sido usados como a base de vários sistemas criptográficos propostos (ver (**TERADA, 2008**)). Algoritmos aleatórios eficientes são dadas para estes dois problemas em um computador quântico hipotético. Estes algoritmos tomam uma série de etapas e é polinomial no tamanho da entrada, por exemplo, o número de dígitos do número inteiro a ser fatorado.

Quando propôs o algoritmo, **Shor** trabalhava na empresa AT&T e desenvolvia pesquisas que apontavam vantagens dos computadores quânticos em relação à máquina de **Turing**. Nesse panorama, **Shor** formulou um algoritmo quântico que permitia decompor um número com muitos algarismos em seus fatores primos. O detalhe fundamental é que o algoritmo de **Shor** realiza essa tarefa em tempos muito menores do que os gastos por algoritmos clássicos (porque é quântico). O problema



Figura 174 – Peter Shor - O algoritmo quântico de fatoração de números primos grandes.

Fonte: en.wikipedia.org.

da fatoração é essencial para os sistemas criptográficos atuais, mas que não trairiam vantagens quanto a inviabilidade computacional útil na criptografia convencional. Notamos, ainda que, os sistemas criptográficos de segurança baseados em chave pública ficarão totalmente obsoletos a partir do momento em que o primeiro computador quântico iniciar o seu funcionamento. É conhecido do ponto de vista teórico, o elevado potencial computacional dos sistemas quânticos.

### 11.2.2 Da teoria dos números ...

O que é número composto? É qualquer número natural que pode ser escrito como resultado da multiplicação entre números primos.

Os números naturais são divididos de muitas maneiras, em outros subconjuntos numéricos. Os mais comuns são: *números pares*, *números ímpares*, *números primos* e os *números compostos*. Os *números compostos* são aqueles que resultam da multiplicação de números *primos*. Para discutir com maior profundidade o que é um *número composto*, é preciso conhecer bem o *conjunto dos números primos*.

Um número natural é *composto* quando tem *mais de dois divisores naturais distintos*. Alguns números ímpares como o 9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, ... são compostos, pois são divisíveis por mais de dois números naturais distintos. Conclusão: Todo o número *inteiro não-primo* e diferente de 1 é *composto*.

**Números primos** - Para ser considerado primo, um número deve ser divisível apenas por si mesmo ou por 1. Dessa maneira, os números primos constituem um subconjunto infinito de números naturais cujos primeiros elementos são:

{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...}

Observe que o **único número par que é primo é o 2**. Isso acontece porque qualquer outro número par é divisível por 2 e, por isso, não é primo.

Observe também que o **número 1, embora seja divisível apenas por si mesmo e por 1, não é um número primo**. Isso acontece por causa do **teorema fundamental da aritmética**, exposto a seguir.

**Teorema fundamental da aritmética** - Esse teorema é a regra matemática que garante que todo número pode ser escrito como um produto de números primos. Observe:

"Todo número natural maior que 1 ou é primo ou pode ser escrito como produto de números primos."

**Números compostos** - Os números compostos são exatamente aqueles que podem ser escritos como produtos de números primos. São exemplos de números compostos:  $4 = 2 \times 2$ ,  $6 = 2 \times 3$ ,  $8 = 2 \times 2 \times 2$  e  $9 = 3 \times 3$ . Observe que os fatores são números primos. Quando não forem, poderão ser decompostos novamente, originando fatores primos. Observe:  $40 = 2 \times 20 = 2 \times 2 \times 10 = 2 \times 2 \times 2 \times 5$ .

```

15360| 2
 7680| 2
 3840| 2
 1920| 2
  960| 2
  480| 2
  240| 2
  120| 2
   60| 2
   30| 2
   15| 3
    5| 5
    1| 210·3·5

```

Figura 175 – A fatoração de números primos.

Fonte: <<https://brasilecola.uol.com.br/o-que-e/matematica/o-que-e-numero-composto.htm>>

Para aqueles que, na decomposição da Figura 175, precisam ver os **critérios de divisibilidade**, consulte o link: <<https://brasilecola.uol.com.br/matematica/criterios-divisibilidade.htm>>.

### 11.2.3 Visão geral do algoritmo de Shor

O algoritmo de **Shor** é um algoritmo quântico que encontra com alta probabilidade a ordem de um elemento  $x \in \mathbb{Z}_n^*$ . Uma de suas aplicações é a construção de um algoritmo que encontra fatores de  $n$ . (FREITAS, 2010)

O algoritmo de **Shor** resolve o problema da fatoração de inteiros em primos e consome **tempo polinomial** no tamanho da entrada. Os detalhes fundamentais do

funcionamento deste algoritmo podem ser encontrados em (CARDONHA; SILVA; FERNANDES, 2004) ou em (SILVA, 2004).

O algoritmo de **Shor** (SHOR, 1994a) (SHOR, 1994b) e (SHOR, 1997) é um algoritmo quântico que, dado um inteiro  $n$  composto ímpar, que não é potência de um número primo, devolve um fator de  $n$  com probabilidade limitada de erro.

As restrições para o valor de  $n$  não representam problema algum. De fato, é trivial encontrar um fator de um número par. Além disso, é fácil desenvolver um algoritmo eficiente que decide, se  $n = a^k$ , para inteiros  $a$  e  $k > 1$ , e que devolve  $a$  e  $k$ , neste caso. Veja o artigo de **Bernstein** (BERNSTEIN, 1998) para mais detalhes.

Um problema cuja complexidade continua em aberto, mesmo após várias décadas de esforço para resolvê-lo, é o **problema da fatoração de inteiros**: dado um inteiro, determinar a sua **fatoração em números primos**. Recentemente, o seu similar próximo, o problema de decidir se um número inteiro é primo ou não, chamado de *problema da primalidade*, teve sua complexidade totalmente definida, com o **algoritmo AKS** de **Agrawal, Kayal e Saxena** (AGRAWAL; KAYAL; SAXENA, 2004). Esse algoritmo mostra que o **problema da primalidade está na classe P**, resolvendo com isso uma questão em aberto há anos. **Não se sabe até hoje, no entanto, se existe um algoritmo eficiente para resolver o problema da fatoração de inteiros!**

O problema computacional que é a fatoração de inteiros para números extremamente grandes (com mais de 100 dígitos decimais) tem motivado diversos estudos devido a sua aplicação em sistemas de criptografia (MOLGORA, 2013). Quando os números são muito grandes não se conhece nenhum algoritmo que resolva eficientemente este problema; uma recente iniciativa de diversos pesquisadores concluída em 2009, de fatorar um número de 232 dígitos (RSA-768) utilizando centenas de máquinas demorou 3 anos e os pesquisadores estimaram que um módulo RSA de 1024 bits demoraria mais ou menos 3000 anos. Apesar disso, não foi provado que nenhum algoritmo eficiente exista. A suposta dificuldade é o núcleo de certos algoritmos criptográficos, como o RSA. Muitas áreas da matemática e da ciência da computação, como a teoria algébrica dos números, as curvas elípticas, a computação distribuída <<https://homepages.dcc.ufmg.br/~nivio/cursos/pa04/seminarios/seminario12/seminario12.html>> ou a **computação quântica**, estão relacionadas com este problema. Na verdade, a dificuldade computacional do problema da fatoração de inteiros tem sido usada de maneira crucial em alguns sistemas criptográficos bem-conhecidos. Se for descoberto um algoritmo eficiente para resolver o problema da fatoração, vários sistemas criptográficos importantes seriam quebrados, incluindo o sistema RSA de chave pública criado por **Rivest, Shamir e Adleman** (RIVEST; SHAMIR; ADLEMAN, 1978).

Ademais, podemos verificar em tempo polinomial, se  $n$  é composto, utilizando o algoritmo AKS. Outra opção é executar *testes de primalidade probabilísticos*, um número suficiente de vezes. Na prática, isso é mais eficiente, pois os testes probabilísticos são, em geral, mais simples e rápidos que o AKS. O teste de **Miller-Rabin** <[https://pt.wikipedia.org/wiki/Teste\\_de\\_primalidade\\_de\\_Miller-Rabin](https://pt.wikipedia.org/wiki/Teste_de_primalidade_de_Miller-Rabin)> ou em (RABIN, 1980) é uma ótima escolha para esta verificação, por ser de fácil implementação e ter complexidade de tempo  $\mathcal{O}(\lg^3 n)$ , com uma constante pequena ocultada pela notação assintótica.



Como  $n$  é produto de no máximo  $\lg n$  inteiros, o algoritmo de **Shor** pode ser utilizado para resolver o problema da fatoração em tempo polinomial no tamanho da entrada.

O algoritmo de *Shor* baseia-se numa *redução do problema da busca de um fator de  $n$  ao problema da busca do período* de uma função. Como a redução utiliza aleatorização, é possível que ela falhe, isto é, que nenhum fator de  $n$  seja encontrado. Pois, a probabilidade de ocorrência deste evento é limitada. Apresentamos essa redução e limitamos a probabilidade de falha.

Apresentamos o algoritmo quântico eficiente para a busca do período da sequência gerada pela *redução*. Seja  $n$  um inteiro composto ímpar que não é potência de primo. Vamos mostrar como reduzir o problema de encontrar um fator de  $n$  ao problema de encontrar o período de uma função. Essa redução utiliza aleatorização, de modo que precisaremos limitar a probabilidade de falha do procedimento.

O algoritmo de **Shor** pode ser visto como:

### Algoritmo Shor ( $n$ )

---

```

1 Escolha um inteiro  $1 < x < n$  aleatoriamente.
2 Se  $\text{mdc}(x, n) > 1$ 
3 —então devolva  $\text{mdc}(x, n)$ 
4 Seja  $r$  o período da função  $f(a) = x^a \text{ mod } n$ 
5 Se  $r$  for ímpar ou  $x^{r/2} \equiv -1 \pmod{n}$ 
6 —então "o procedimento falhou"
7 devolva  $\text{mdc}(x^{r/2} + 1, n)$ 

```

---

O que vem a seguir depende de se conhecer a seguinte notação ([ATKINSON, 2001](#)):

- $\mathbb{Z}_n$  conjunto dos inteiros módulo  $n$ :  $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$ .
- $\mathbb{Z}_n^*$  conjunto dos elementos  $x$  de  $\mathbb{Z}_n$  não nulos, tais que  $\text{mdc}(x; n) = 1$ .
- $r = \text{ord}_n(x)$ ,  $r$  é o menor natural  $a$  tal que  $x^a \equiv 1 \pmod{n}$ ;  $r$  é dito ser a ordem de  $x$  módulo  $n$ , ou também a ordem de  $x$  em  $\mathbb{Z}_n^*$ .
- $x^a \text{ mod } n$  é exponenciação modular.

Note que o algoritmo de **Shor** utiliza **um único passo quântico**: o cálculo do período da função na linha 4. Uma rotina quântica para encontrar o período de *funções exponenciais modulares* é o núcleo do algoritmo de **Shor** no passo 4. A rotina quântica para encontrar o período de  $f(a) = x^a \text{ mod } n$  emprega um par de registradores quânticos  $|x_1\rangle$  e  $|x_2\rangle$ . Veja ([ATKINSON, 2001](#)). A determinação  $r = \text{ord}_n(x)$  é a parte mais difícil do algoritmo 2.1.1 em ([ATKINSON, 2001](#)) para obtenção de fatores de  $n$  não triviais.

### Ordem como Período da função $f(a) = x^a \text{ mod } n$ -

Escolhendo aleatoriamente a  $x \in \mathbb{Z}_n^*$ , sabemos qual a probabilidade de que  $r = \text{ord}_n(x)$  seja adequada para a determinação de fatores não-triviais de  $n$ . Para a determinação de  $r$  temos o algoritmo 2.1.5 em ([ATKINSON, 2001](#)). Uma outra

maneira de determinar  $r$  é calcular o período da função  $f(a) = x^a \bmod n$ . O período de funções  $f(a) = x^a \bmod n$  está relacionado com a ordem  $\text{ord}_n(x)$  de elementos  $x$  de  $\mathbb{Z}_n^*$  (elementos de  $\mathbb{Z}_n$  não nulos, tais que  $\text{mdc}(x; n) = 1$ );

A demonstração dos vários teoremas relevantes na Teoria dos Números, pode ser encontrada em (MILIES; COELHO, 1998).

Da *Transformada de Fourier Discreta*, temos a *transformada de Fourier clássica* e sua utilização na determinação do período de funções, e da transformada de Fourier quântica e o modo de aplicá-la sobre registradores quânticos. (ATKINSON, 2001).

Agora vamos mostrar que, se a redução devolve uma resposta, ela está correta. Depois vamos delimitar superiormente a probabilidade de falha deste procedimento, isto é, a probabilidade de o algoritmo terminar na linha 6.

Começamos observando que, se o algoritmo executa a linha 3, então o valor devolvido, de fato, é um fator de  $n$ .

Já se  $\text{mdc}(x, n) = 1$ , então  $x$  está em  $\mathbb{Z}_n^*$ , o grupo multiplicativo módulo  $n$ , de modo que a função  $f(a) = x^a \bmod n$  é periódica com período dado pela ordem de  $x$ , módulo  $n$ . Isto é, o período  $r$  é o tamanho do subgrupo de  $\mathbb{Z}_n^*$  gerado por  $x$ . Equivalentemente,  $r$  é o menor inteiro positivo tal que  $x^r \equiv 1 \pmod{n}$ .

Para se estudar a prova do algoritmo de **Shor**, o leitor deve passar por três etapas:

1. Redução à busca do período de uma função (SILVA, 2004);
2. A busca do período (o passo quântico) (SILVA, 2004);
3. A transformada quântica de **Fourier** (SILVA, 2004).

Nos trabalhos de (SILVA, 2004) e (CARDONHA; SILVA; FERNANDES, 2004), apresenta-se essa redução e uma delimitação superior para a probabilidade de falha. É também mostrado o procedimento matemático para a busca do período da sequência gerada pela redução. E a utilização da *transformada quântica de Fourier*, que pode ser implementada.

## 11.3 Algoritmo Quântico de Lov Grover - 1996

Um outro algoritmo quântico que merece destaque foi proposto pelo indiano **Lov Grover** (1961-). Trata-se de um cientista indiano-americano, originador do algoritmo de busca em "base de dados" usado em computação quântica. Enquanto trabalhava nos laboratórios de pesquisa *Bell*, nos Estados Unidos. **Grover**, em 1996, propôs um algoritmo de busca, o qual, como o próprio nome já sugere, realiza a tarefa de buscar numa base de dados, encontrando itens que tenham certas propriedades desejadas. Estamos acostumados a utilizar algumas espécies de sistemas como esses, quando usamos a Internet. Assim, como o algoritmo de **Shor**, a vantagem computacional apresentada pelo algoritmo de **Grover** foi excelente, pois em geral, numa determinada tarefa onde classicamente precisamos fazer  $N$  buscas, quanticamente são necessárias  $\sqrt{N}$ , que é um número muito menor. (GROVER, 1996)

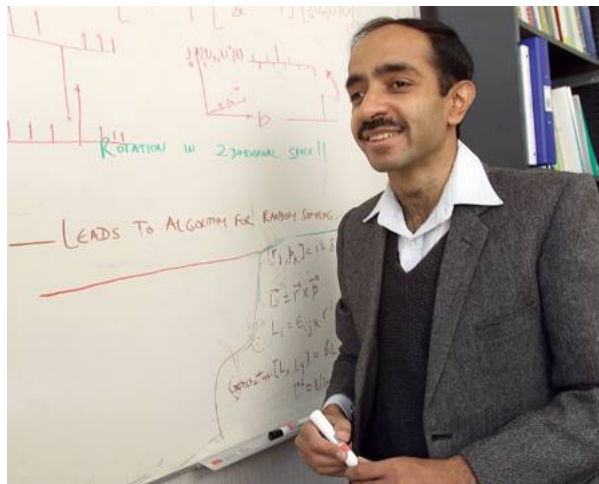


Figura 176 – Lov Grover - O inventor do algoritmo de busca quântico em uma base de dados.

Fonte: Google Images - [www.kennislink.nl](http://www.kennislink.nl).

A título de ilustração, considere uma tarefa na qual classicamente necessitaríamos 10000 buscas; dessa maneira, quanticamente seriam necessárias apenas 100 buscas. O algoritmo de **Grover** pode ser aplicado com sucesso em problemas práticos da biologia molecular e engenharia genética.

### O algoritmo:

- Problema Encontrar um valor  $a \in A$  em um espaço  $\mathcal{H}$  (banco de dados, vetor ou outra estrutura/fonte de dados).
- $\mathcal{H}$  possui  $N = 2^n$  entradas (posições).
- **Grover:**
  - São necessário  $n$  *qubits* para endereçar o espaço (mais o número de *qubits* para representar os elementos do espaço).
  - São necessários  $\mathcal{O}(\sqrt{N})$  passos.

Em computação quântica, O algoritmo de **Grover** ou Algoritmo de Busca  $\mathcal{O}(n^{1/2})$  é um algoritmo quântico que encontra com alta probabilidade a entrada exclusiva para uma função de caixa preta que produz um valor de saída específico, usando apenas avaliações da função  $\mathcal{O}(\sqrt{N})$ , em que  $N$  é o tamanho do domínio da função. O algoritmo quântico **Grover** permite uma aceleração enorme em algoritmos de busca que afeta a segurança de muitos criptosistemas, incluindo AES (Advanced Encryption Standard).

O problema análogo na computação clássica não pode ser resolvido em menos de  $\mathcal{O}(N)$  avaliações (porque, no pior dos casos,  $N$ , o  $N$ -th membro do domínio pode ser o membro correto). Aproximadamente na mesma época em que **Grover** publicou seu algoritmo, **Bennett, Bernstein, Brassard e Vazirani** provaram que qualquer solução quântica para o problema precisa avaliar a função  $\Omega(\sqrt{N})$  vezes. O

algoritmo de **Grover** é *assintoticamente ótimo*.

Foi demonstrado que um computador quântico de *variável oculta não local* poderia implementar uma pesquisa sobre um banco de dados com  $N$  itens no máximo  $\mathcal{O}(\sqrt{3N})$  passos. Isso é mais rápido que a ordem de  $\mathcal{O}(\sqrt{N})$  passos, dados pelo algoritmo de **Grover**. Porém nenhum dos métodos de busca permitirá que computadores quânticos resolvam problemas *NP-Completo*s em tempo polinomial.

Ao contrário de outros algoritmos quânticos, que podem fornecer aceleração exponencial sobre suas contrapartes clássicas, o algoritmo de **Grover** fornece apenas um aumento de velocidade quadrático. No entanto, mesmo a aceleração quadrática é considerável quando  $N$  é grande. O algoritmo de **Grover** poderia forçar brutalmente uma chave criptográfica simétrica de 128 bits em aproximadamente  $2^{64}$  iterações, ou uma chave de 256 bits em aproximadamente  $2^{128}$  iterações. Como resultado, às vezes é sugerido que os comprimentos de chave simétrica sejam duplicados para proteger contra futuros ataques quânticos.

Como muitos algoritmos quânticos, o algoritmo de **Grover** é probabilístico no sentido de dar a resposta correta com uma probabilidade menor que 1. Embora tecnicamente não haja limite superior no número de repetições que podem ser necessárias antes que a resposta correta seja obtida, o número esperado de repetições é um fator constante que não cresce com  $N$ . O artigo original de **Grover** descreveu o algoritmo como um algoritmo de busca de banco de dados, e essa descrição ainda é comum. O banco de dados nesta analogia é uma tabela de todas as saídas da função, indexada pela entrada correspondente.

Embora o propósito do algoritmo de **Grover** seja usualmente descrito como "pesquisar numa base de dados", pode ser mais preciso descrevê-lo como "inverter uma função". Na verdade, como um *oráculo* de um banco de dados não estruturado requer pelo menos complexidade linear, o algoritmo não pode ser usado para bancos de dados reais. Se uma função  $y = f(x)$  pode ser avaliada por um computador quântico, o algoritmo de **Grover** calcula  $x$  quando um  $y$  for dado. A inversão de uma função está relacionada à pesquisa de um banco de dados, porque poderíamos criar uma função que produzisse um valor específico de  $y$ , se  $x$  corresponde a uma entrada desejada no banco. O algoritmo de **Grover** também pode ser usado para estimar a média e a mediana de um conjunto de números e para resolver o *problema de colisão*, como no cálculo de uma função *hash*. O algoritmo de **Grover** poderia ser usado para fazer engenharia reversa de funções *hash* criptográficas, permitindo que um invasor encontre a senha da vítima ou gere uma série de blocos falsificados.

A Figura 177 mostra o circuito quântico para o algoritmo de **Grover**:

Atualmente, um algoritmo de busca em listas desordenadas possui a complexidade de  $\mathcal{O}(N)$ , o algoritmo de Grover consegue realizar buscas em listas desordenadas com complexidade de  $\mathcal{O}(\sqrt{N})$ . O algoritmo inverte o sinal do *qubit* quando  $f(\text{qubit}) = 1$ , e não altera o *qubit*, se  $f(\text{qubit}) = 0$ . O circuito pode ser visto na Figura 177.  $U_F$  depende da  $f(x)$ , ou seja, depende de qual número a busca tem que retornar. A matriz  $D$  é uma matriz de controle como podemos ver na Figura 178:

Usando esse circuito na Figura 177 podemos obter o resultado esperado da busca na complexidade  $\mathcal{O}(\sqrt{N})$ .

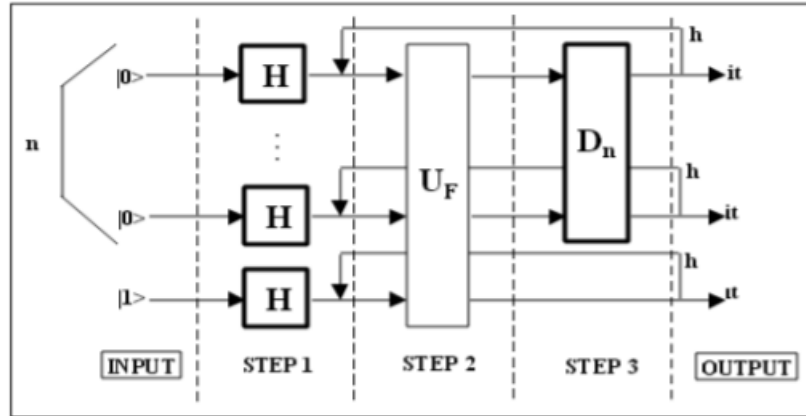


Figura 177 – Circuito quântico para o algoritmo de Grover.

Fonte: <[https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin\\_ArqQuant.pdf](https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin_ArqQuant.pdf)>

$D_n$	$ 0..0\rangle$	$ 0..1\rangle$	...	$ i\rangle$	...	$ 1..0\rangle$	$ 1..1\rangle$
$ 0..0\rangle$	$-1+1/2^{n-1}$	$1/2^{n-1}$	...	$1/2^{n-1}$	...	$1/2^{n-1}$	$1/2^{n-1}$
$ 0..1\rangle$	$1/2^{n-1}$	$-1+1/2^{n-1}$	...	$1/2^{n-1}$	...	$1/2^{n-1}$	$1/2^{n-1}$
...	...	...	...	...	...	...	...
$ i\rangle$	$1/2^{n-1}$	$1/2^{n-1}$	...	$-1+1/2^{n-1}$	...	$1/2^{n-1}$	$1/2^{n-1}$
...	...	...	...	...	...	...	...
$ 1..0\rangle$	$1/2^{n-1}$	$1/2^{n-1}$	...	$1/2^{n-1}$	...	$-1+1/2^{n-1}$	$1/2^{n-1}$
$ 1..1\rangle$	$1/2^{n-1}$	$1/2^{n-1}$	...	$1/2^{n-1}$	...	$1/2^{n-1}$	$-1+1/2^{n-1}$

Figura 178 – A matriz D do circuito quântico do algoritmo de Grover.

Fonte: <[https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin\\_ArqQuant.pdf](https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin_ArqQuant.pdf)>

## 11.4 O problema de Deutsch-Jozsa - 1992

O algoritmo **Deutsch-Jozsa** generaliza o trabalho anterior (1985) de **David Deutsch**, que forneceu uma solução para o caso simples descrito a seguir.

Este foi o primeiro algoritmo (DEUTSCH, 1985), onde foi mostrado que um computador quântico tem vantagem em um computador clássico. O problema de **Deutsch** (também pode ser encontrado em (SILVA, 2004) na seção 2.5) consiste em saber, se uma determinada função  $f(x)$  é constante ou balanceada. Uma função constante é quando  $f(x)$  é igual para qualquer  $x$ , e uma função balanceada é quando  $f(x)$  é diferente (CABRAL; LIMA; LULA, 2004), isso pode ser visto melhor na tabela 180:

Para um computador clássico essa operação teria que ser feita duas vezes, testando  $x = 0$  e  $x = 1$ . Para um computador quântico essa operação teria que ser feita apenas uma vez. A Figura 181 apresenta o circuito feito para o algoritmo resolver o problema de **Deutsch**.

Para se resolver o problema com certeza no modelo clássico, são necessárias duas aplicações de  $f$ : é preciso usar a caixa preta de  $f$  duas vezes, para as entradas 0 e 1. Já no modelo quântico, este problema pode ser resolvido utilizando-se apenas uma chamada à caixa preta. Vamos mostrar um algoritmo quântico, devido a **Cleve, Ekert, Macchiavello e Mosca** (CLEVE et al., 1998), que resolve o problema no

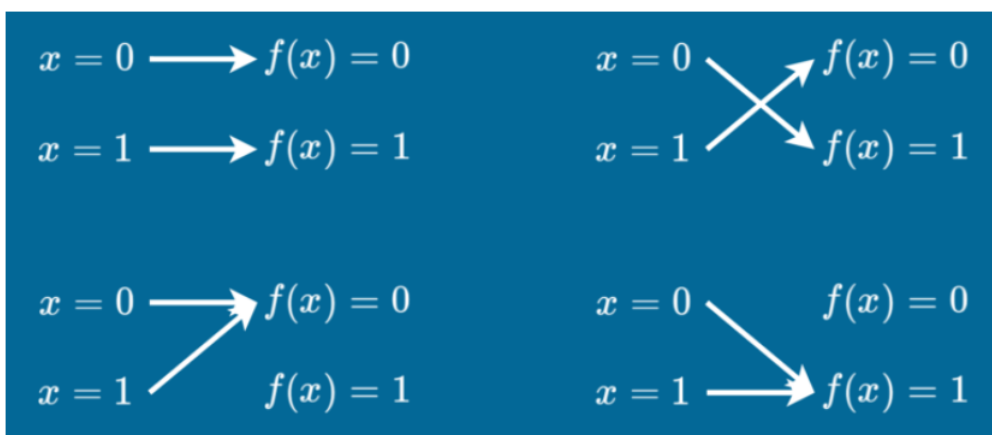


Figura 179 – Função constante ou balanceada ?

Fonte: <<http://dkopczyk.quantee.co.uk/deutschs-algorithm/>>

x	f1(x)	f2(x)	f3(x)	f4(x)
0	1	0	0	1
1	1	0	1	0

Figura 180 – Exemplo de função constante ou balanceada.

Fonte: <[https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin\\_ArqQuant.pdf](https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin_ArqQuant.pdf)>

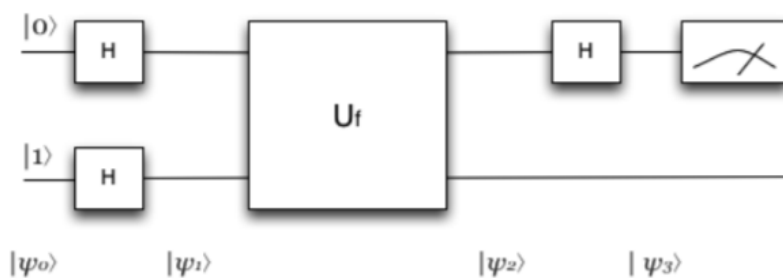


Figura 181 – Circuito quântico para o algoritmo de Deutsch.

Fonte: <[https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin\\_ArqQuant.pdf](https://www.dcce.ibilce.unesp.br/~aleardo/cursos/arqcomp/Semin_ArqQuant.pdf)>

modelo quântico com uma única chamada à caixa preta.

Apesar de pouco uso prático, é um dos primeiros exemplos de um algoritmo quântico que é exponencialmente mais rápido que qualquer algoritmo clássico determinístico possível, e é a inspiração para o **Algoritmo de Simon**, que é, por sua vez, a inspiração para o **Algoritmo de Shor**. É também um *algoritmo determinístico*, o que significa que sempre produz uma resposta, e essa resposta está sempre correta.

**Algoritmo de Simon** <[https://en.wikipedia.org/wiki/Simon%27s\\_problem](https://en.wikipedia.org/wiki/Simon%27s_problem)> - Na **teoria da complexidade computacional e computação quântica** (ver em (CARDONHA; SILVA; FERNANDES, 2004)), o **problema de Simon** é um problema computacional que pode ser resolvido exponencialmente mais rápido em um computador quântico do que em um computador clássico (ou tradicional). Embora o problema em si seja de pouco valor prático, pode-se provar que um algoritmo quântico pode resolver este problema exponencialmente mais rápido do que qualquer algoritmo clássico conhecido. (ARORA; BARAK, 2007)

## Classes de Complexidade

Classe dos problemas resolvidos em

- P: tempo polinomial no modelo clássico
- BPP: tempo polinomial no modelo clássico e probabilidade de falha limitada por constante
- PSPACE: espaço polinomial no modelo clássico
- EQP: tempo polinomial no modelo quântico
- BQP: tempo polinomial no modelo quântico e probabilidade de falha limitada por constante

Pode-se provar:

$$P \subseteq EQP \subseteq BPP \subseteq BQP \subseteq PSPACE$$

Figura 182 – Relações entre classes de complexidade clássicas e quânticas.

Fonte: (CARDONHA; SILVA; FERNANDES, 2004) e em <<https://pt.wikipedia.org/wiki/BQP>>

O problema (**Simon**) é definido no *modelo de complexidade da árvore de decisão* <[https://pt.wikipedia.org/wiki/Modelo\\_de\\_árvore\\_de\\_decis~ao](https://pt.wikipedia.org/wiki/Modelo_de_árvore_de_decis~ao)> ou *complexidade da consulta* (KOIRAN; NESME; PORTIER, 2005), e foi concebido por **Daniel Simon** em 1994 (SIMON, 1994). **Simon** exibiu um algoritmo quântico, geralmente chamado **algoritmo de Simon**, que resolve o problema exponencialmente mais rápido que qualquer algoritmo clássico determinístico ou probabilístico, exigindo exponencialmente menos tempo de computação (ou, mais precisamente, consultas) do que o melhor algoritmo probabilístico clássico.

Esse problema produz uma separação *oracle* entre as classes de complexidade *BPP*

e  $BQP$ , diferentemente da separação fornecida pelo **algoritmo Deutsch-Jozsa**, que separa  $P$  e  $EQP$  (na teoria da complexidade computacional,  $P$  é uma classe de complexidade fundamental, que contém todos os problemas de decisão que podem ser resolvidos por uma *máquina de Turing determinística* usando uma quantidade polinomial de tempo de computação; na teoria da complexidade computacional,  $EQP$ , que significa tempo polinomial quântico exato, é a classe de problemas de decisão que pode ser resolvida por um computador quântico que produz a resposta correta com probabilidade 1 e é executado em tempo polinomial; é o análogo quântico da classe de complexidade  $P$ ).

O **algoritmo de Simon** também foi a inspiração para o algoritmo de **Shor**. Ambos os problemas são casos especiais do problema do *subgrupo abeliano oculto* (KOIRAN; NESME; PORTIER, 2007), que agora é conhecido por ter algoritmos quânticos eficientes.

Uma separação *oracle*, neste contexto, é visto como uma entidade capaz de responder a uma coleção de perguntas, e é geralmente representado como um subconjunto  $A$  dos números naturais. Em *teoria da computação*, uma *máquina oráculo* é uma máquina abstrata usada para estudar problemas de decisão. Ela pode ser vista como uma máquina de **Turing** com uma caixa preta, chamada de *oráculo*, que é capaz de decidir alguns problemas de decisão em uma única operação. O problema pode ser de qualquer classe de complexidade. Até mesmo problemas indecidíveis, como o problema da parada, podem ser decididos nela.

## 11.5 Para saber mais sobre Shor

Quantum Computation and Quantum Information. [S.l.]: por Nielsen, M. e I. Chuang (2000) Cambridge University Press, 2000.

Mosca, M. (2008). Quantum Algorithms. <[arXiv:0808.0369](https://arxiv.org/abs/0808.0369)>

Shor's Algorithm por Roger Herrigel e Wojciech De Roeck, em 14 de abril de 2008

Photons set fresh quantum computing record por Jacob Aron, em 23 de outubro de 2012

Computação Quântica: O algoritmo de fatoração de Shor - (MARCEL K. DE CARLI SILVA) <https://bcc.ime.usp.br/tccs/2004/magal/mac499-monografia.pdf>

## 11.6 Para saber mais sobre Grover

Lecture 4: Grover's Algorithm do curso: "Quantum Computation (CMU 15-859BB, Fall 2015)" em 21 de setembro de 2015, por John Wright e Tom Tseng. Disponível em: <<https://www.cs.cmu.edu/~odonnell/quantum15/lecture04.pdf>>

Quantum Computation: A cryptography armageddon? por Cassius Puodzius, publicado por WLSecurity (2016): Disponível em <<http://www.welivesecurity.com/2016/06/14/quantum-computation-cryptography-armageddon/>>



An Introduction to Quantum Algorithms por Emma Strubell (2011): Disponível em:  
<[https://people.cs.umass.edu/~strubell/doc/quantum\\_tutorial.pdf](https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf)>

The strengths and weaknesses of quantum computation. *SIAM Journal on Computing*, 26. arXiv:quant-ph/9701001. Acessível livremente. doi:10.1137/s0097539796300933.

Quantum Computing and Hidden Variables (PDF): Disponível em:  
<<http://www.scottaaronson.com/papers/qchvpra.pdf>>

Grover vs. McEliece (PDF): Disponível em:  
<<http://cr.yp.to/codes/grovercode/>>

Is Quantum Search Practical? Disponível em:  
<<https://web.eecs.umich.edu/~imarkov/pubs/jour/cise05-grov.pdf>>

In Wikimedia Foundation: Disponível em:  
<[https://pt.wikipedia.org/wiki/Algoritmo\\_de\\_Grover](https://pt.wikipedia.org/wiki/Algoritmo_de_Grover)>

## 11.7 Para saber mais sobre Deutsch

D. Deutsch and R. Jozsa, Rapid solutions of problems by quantum computation, *Proceedings of the Royal Society of London A*. 439: 553 (1992)

N. S. Yanofsky and M. A. Mannucci, *Quantum Computing for Computer Scientists*, Cambridge University press (2008).

Lecture 5: A simple searching algorithm; the Deutsch-Jozsa algorithm:  
<<https://cs.uwaterloo.ca/~watrous/LectureNotes/>>

Quantum Algorithms Tutorial - Ronald de Wolf, <<https://2017.pqcrypto.org/school/slides/qalgotutorial17handout.pdf>>

## 11.8 Para saber mais ... Teoria da Complexidade Quântica

E. Bernstein and U. Vazirani. Quantum complexity theory. In *Proceedings of the 25th ACM Symposium on the Theory of Computation*, pages 11-20, New York, 1993. ACM Press.

E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411-1473, 1997.

## Criptografia Quântica

A segurança das transações bancárias, do comércio eletrônico e das mensagens militares assenta em sistemas de criptografia bastante seguros. Mas, bastante seguros não é o mesmo que absolutamente seguros. A segurança dos métodos atuais se baseia em problemas computacionais difíceis. Mas, basta que surja uma nova geração de computadores - os chamados *computadores quânticos* - em que muitos cientistas pesquisam para sua construção - para que o mundo da comunicação, tal como hoje o conhecemos, possa entrar em colapso. Se algum desses avanços revolucionários for de repente alcançado, deverão ser revistos todos os seus sistemas de comunicação, porque com computadores quânticos, sistemas de segurança serão certamente quebrados, já que poderá haver brechas de segurança na comunicação criptografada pelos métodos atuais usados. Será o colapso da sociedade da informação.

Neste contexto, o que todo mundo procura é uma nova forma de criptografia que seja verdadeiramente segura. Um novo sistema que será completamente inviolável, basear-se-á **nas leis mais profundas da matéria**, ou seja, **nas leis que regem a incerteza do mundo quântico**. **A absoluta impossibilidade de se conhecer o comportamento das partículas elementares, será a garantia de segurança das mensagens**. Uma técnica muito promissora é a **criptografia quântica**, como veremos a seguir.

### 12.1 Algoritmos criptográficos

Nos algoritmos modernos, o segredo de uma mensagem encontra-se na *chave*, que é um parâmetro utilizado na cifragem e decifragem de uma mensagem. Quanto maior for o tamanho da chave, espera-se que seja mais difícil quebrá-la.

Para melhor entendimento e seguindo a literatura, chamemos de *Alice* quem quer mandar uma mensagem privada e *Bob* quem vai recebê-la. E denominemos *Eva*, um intruso tentando ler esta mensagem secreta.

Figura 183 – Algoritmos criptográficos em geral.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:  
<<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>>

Nos *algoritmos simétricos*, também conhecidos como de *chave privada*, a mesma chave é utilizada tanto na cifragem como na decifragem. Desta forma, Alice e Bob precisam combinar uma chave previamente. Nas transações comerciais e bancárias realizadas através da internet, a utilização de apenas esta chave é impraticável, sendo necessário um *algoritmo assimétrico* ou de *chave pública*, como veremos adiante.

Exemplos de algoritmos de chave privada são o *One Time Pad* (uma cifra simples mas incondicionalmente segura, inventada em 1917 por Gilbert Vernam) e a cifra *DES* (Data Encryption Standard, adotada em 1976 e que continua sendo o padrão oficial americano para cifragem).

A cifra One Time Pad baseia-se na operação XOR (OU exclusivo), como indica a tabela abaixo. O processo de decifragem é análogo.

mensagem original	0	1	1	0	1
CHAVE	1	0	0	0	1
mensagem cifrada	1	1	1	0	0

Tabela 1. Cifra One Time Pad

Podemos utilizar uma chave de tamanho inferior ao da mensagem, pois será mais fácil distribuir uma chave quanto menor esta for. Mas isso deixará brechas para um criptoanalista experiente, que poderá decifrá-la. Caso a chave utilizada no One Time Pad seja aleatória e do tamanho da mensagem, temos uma *segurança incondicional*: prova-se que não há como decifrá-la de forma alguma. Mas o problema de distribuição de chaves permanece: para mandar uma mensagem de tamanho  $n$  com uma segurança incondicional, Alice e Bob precisam combinar previamente uma chave de tamanho  $n$ , o que é inviável para a maioria das aplicações, principalmente quando há um grande fluxo de mensagens.

Num *algoritmo assimétrico*, a chave utilizada na cifragem é diferente daquela utilizada na decifragem. Desta forma, não há a necessidade de Alice e Bob combinarem uma chave previamente, eliminando o problema da distribuição de chaves. A segurança desse algoritmo se baseia em problemas computacionalmente difíceis, como a fatoração de um número razoavelmente grande em seus fatores primos, onde destacamos o algoritmo RSA, que é um dos mais utilizados na atualidade.

Caso haja um grande crescimento do poder computacional, onde destacamos pesquisas com Computadores Quânticos, estes algoritmos não serão mais seguros. Um computador pessoal dos dias atuais demoraria 100 mil bilhões de anos para fatorar um número de 600 dígitos decimais, o que seria realizado em poucos minutos num computador quântico, caso possa ser construído.

Figura 184 – Algoritmos criptográficos - a cifra *One Time Pad*.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:

<<http://www.bibl.ita.br/ixencia/artigos/FundDanielNobuo.pdf>>

## 12.2 Princípios da mecânica quântica - a polarização de fótons

A mecânica quântica nos diz que a luz apresenta, tanto uma natureza corpuscular, quanto ondulatória. Experimentos como o *Efeito Fotoelétrico* (Einstein) e a *Radiação Térmica de um Corpo Negro* (Planck) mostram a natureza corpuscular da luz, nos dizendo que a luz é formada por fótons, partículas elementares indivisíveis de massa igual a zero. Além desses fenômenos, temos a polarização, que mostra a natureza ondulatória, a qual uma onda luminosa consiste de dois campos perpendiculares que variam no tempo: o campo elétrico  $E$  e o campo magnético  $B$ . O plano de polarização é constituído do plano que contém  $E$  e a direção de propagação da onda. Desta forma podemos atribuir uma polarização (qualquer medida em graus) a um fóton. Por exemplos, diferentes planos de polarização, tais como  $0^\circ$ ,  $45^\circ$ ,  $90^\circ$  e  $135^\circ$  de um fóton são ilustradas na Figura 185:

Dado uma fóton podemos mudar sua polarização com a utilização de polarizadores, como cristais de calcita ou óculos de sol. Filtros polaróides deixam passar fótons, como na Figura 186, cuja polarização seja igual a da "fenda" do filtro e absorvem os fótons cujo plano de polarização seja perpendicular a essa.



Figura 185 – Diferentes planos de polarização de um fóton.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:  
<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>

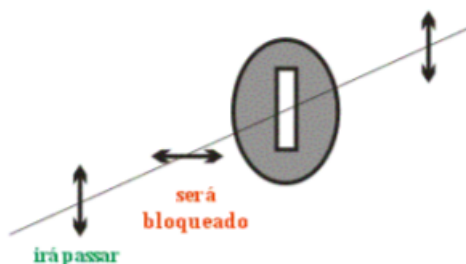


Figura 186 – Um exemplo de filtro polaroide.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:  
<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>

Caso o fóton apresente uma polarização genérica  $\theta$  em relação à fenda do polarizador, a probabilidade do fóton passar é  $P = \cos^2\theta$ , expressão conhecida como *Postulado de Redução de von Neumann*. E caso ele passe, sua polarização será a mesma do polarizador. Por exemplo, se  $\theta = 45^\circ$ , a probabilidade será de 50% do fóton passar e adquirir polarização igual a da fenda do polarizador.

Um fato notável e que exemplifica o **Princípio da Incerteza de Heisenberg** é a impossibilidade da determinação exata da polarização do fóton. Para termos alguma informação sobre a polarização do fóton, precisamos de um filtro polarizador. Caso o fóton não passe por este, apenas podemos concluir que ele não foi polarizado paralelamente à fenda do polarizador. E caso ele passe, apenas podemos concluir que ele não foi polarizado perpendicularmente à fenda. Pois se não ele não iria passar. Com qualquer outra polarização, há uma probabilidade do fóton passar. O **Princípio da Incerteza de Heisenberg**, de uma forma geral, afirma que **não podemos obter todas as informações que descrevem uma partícula subatômica**, não sendo possível, neste caso, determinar a polarização exata de um fóton específico, pois uma observação quântica causa a perturbação no momento da medida.

## 12.3 Um protocolo de bases conjugadas - BB84

Vejamos que de um modo geral, o protocolo utiliza um canal quântico. Alice envia fótons polarizados para Bob, que os mede segundo um polarizador. E pelo canal público eles transmitem mensagens necessárias para a obtenção da chave  $k$ . Sendo que essas mensagens podem ser lidas por um espião qualquer sem afetar a segurança do protocolo. Utiliza-se quatro polarizações:  $0^\circ$  e  $45^\circ$  para representar o bit 0, e  $90^\circ$  e  $135^\circ$  para representar o bit 1, conforme indicado na Figura 187.

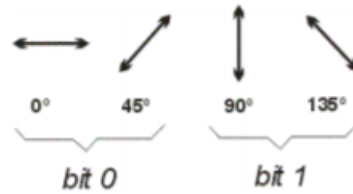


Figura 187 – Exemplo de polarizações referentes aos bits 0 e 1, no protocolo BB84.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:

<<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>>

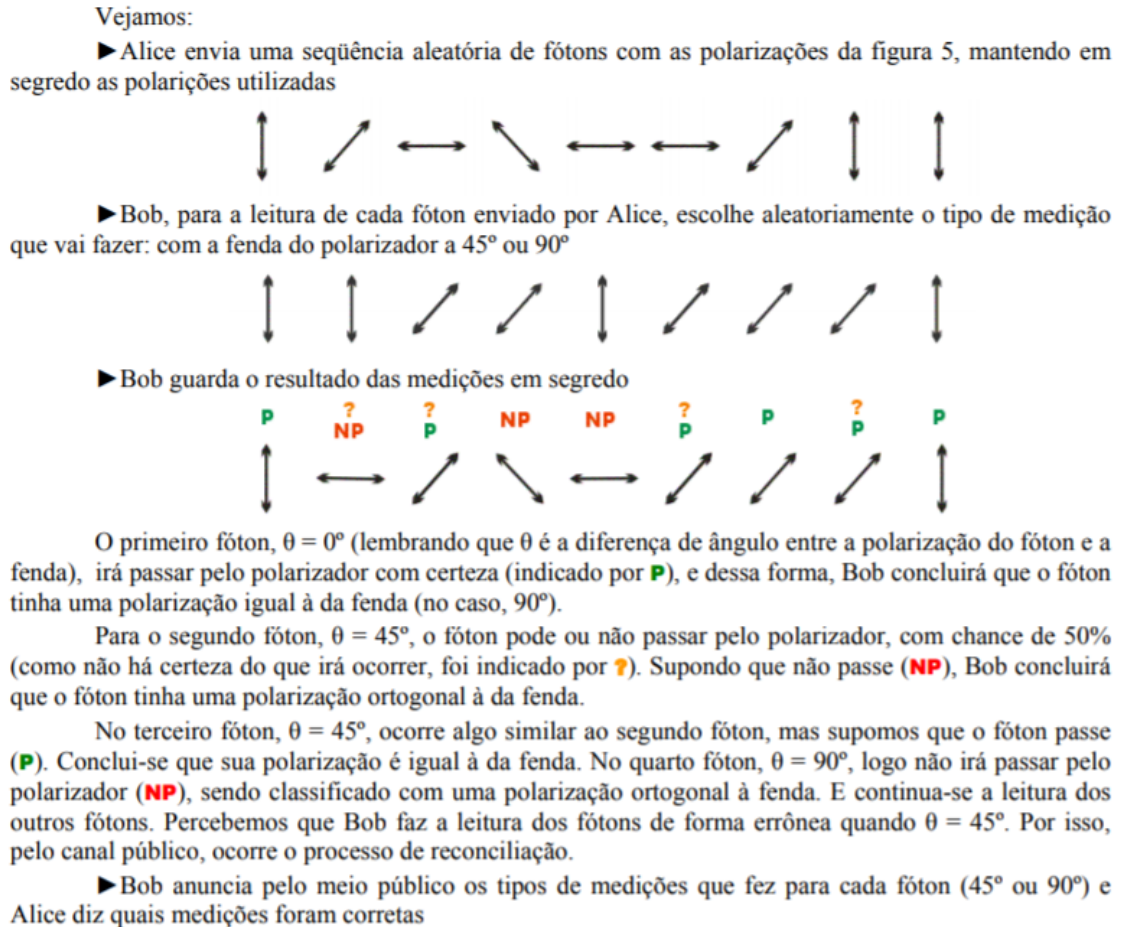


Figura 188 – Explicação do funcionamento do protocolo BB84.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:

<<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>>

## 12.4 A presença de um intruso

O intruso chamar-se-á Eva. Caso Eva tente ler os fótons que Alice enviou, ela não conseguirá ler todos os fótons corretamente: ela apenas sabe que foram enviados fótons com polarizações  $0^\circ$  e  $45^\circ$  para representar o bit 0, e  $90^\circ$  e  $135^\circ$  para representar o bit 1. Utilizando um polarizador, ela irá ter uma leitura correta de no máximo 75% dos bits enviados. Alguns tipos de ataques estão especificados

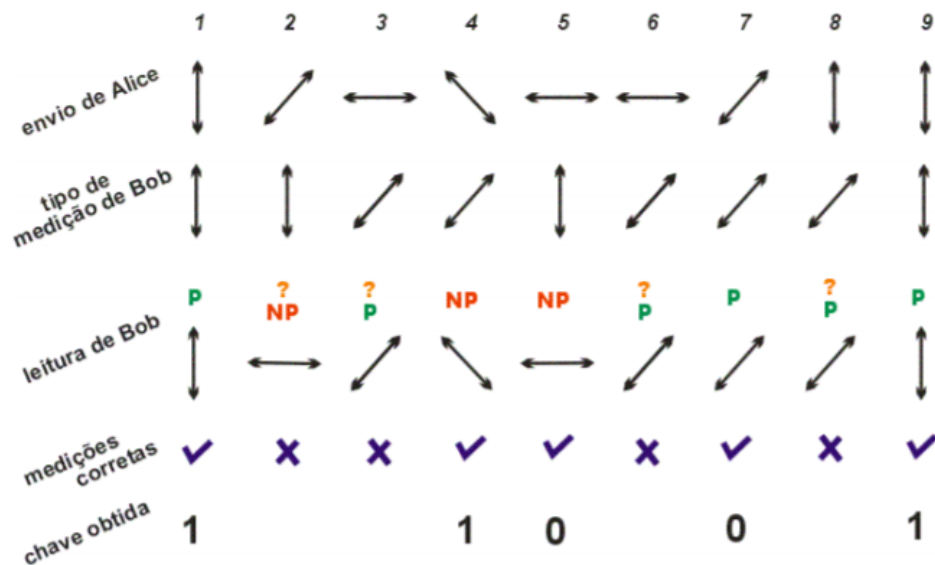


Figura 189 – Passos do protocolo até a obtenção da chave  $k$ .

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:

<<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>>

Para o fóton 1 no caso acima, Bob diz para Alice: “medição com fenda a 90°”. Como Alice sabe a polarização de cada fóton que enviou, ela diz a Bob que a medição foi correta para este fóton (✓). Já para o fóton 2, Bob realizou uma medição com a fenda a 90°, e como o fóton original apresenta um desvio de 45° em relação à fenda, a medição foi errada (✗): a polarização de 45° foi medida como 0°. Alice, sabendo que  $\theta = 45^\circ$  neste caso, diz para Bob que a medição está errada. Esse processo de reconciliação ocorre para toda a seqüência.

Para os fótons cuja medição foi correta (metade da seqüência), Alice e Bob convertem as respectivas polarizações em bits, como indicado pela figura 5, obtendo uma chave. Neste caso ilustrativo com poucos fótons, a chave obtida foi **11001**: essa chave claramente irá ser igual para os dois, caso não haja erros de transmissão ou um intruso. Os erros de transmissão costumam ser baixos (inferiores a 3%) e são causados por ruídos no canal quântico ou pelo desalinhamento dos polarizadores.

Figura 190 – Explicando os passos do BB84.

Fonte: Daniel Nobuo Uno/Antonio Cândido Faleiros em:

<<http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>>

em (KOWADA, 1999) (pg. 28-33). Desta forma, Eva terá de enviar fótons para Bob, e 25% da leitura dos bits de Bob, irão diferir dos de Alice.

Bob, sem saber que Eva leu e reenviou os fótons, faz a leitura dos fótons e o processo de reconciliação normal, obtendo uma chave que difere 25% dos bits de Alice. Desta forma, Alice e Bob anunciam alguns bits da chave para conferi-los. Caso haja uma taxa de erros relativamente alta, provavelmente há um intruso. Caso os erros sejam baixos, eles descartam da chave alguns bits que foram anunciados publicamente.

Pode ser que uma baixíssima porcentagem da chave esteja incorreta devido a erros de transmissão e há procedimentos matemáticos para corrigi-los. Há outros procedimentos na amplificação da privacidade da chave, como pode ser visto em (KOWADA,

1999), pg. 24-27. Dessa forma Alice e Bob compartilham uma chave com privacidade.

O assunto da criptografia quântica começa com as histórias de **Stephen Wiesner** até chegarmos a **Charles Bennett**, onde o tema começou em 1984.

## 12.5 Histórias de Stephen Wiesner ...

As histórias contadas neste parágrafo foram extraídas do livro *The Code Book*, de **Simon Singh** (SINGH, 2000) ou em (RIGOLIN; RIEZNIK, 2005). Trata-se de uma pessoa que estava à frente de seu tempo: **Stephen Wiesner** (1942-), um físico pesquisador que atualmente vive em Israel. Ele recebeu seu diploma de graduação de *Brandeis University* (Boston, USA). Como um estudante de pós-graduação na *University of de Columbia* em Nova York, no final dos anos 1960 e início dos anos 1970, ele descobriu várias das ideias mais importantes da teoria da informação quântica, incluindo:

- *Quantum money* (que levou ao trabalho da distribuição de chaves quânticas por Bennett-Brassard) (BENNETT; BRASSARD, 1984).
- *Quantum multiplexing* (multiplexação quântica), o mais antigo protocolo do tipo *Oblivious Transfer* (WIESNER, 1983). Em criptografia, um *Oblivious Transfer* (OT) é um tipo de protocolo no qual um remetente transfere uma, de potencialmente muitas informações para um receptor, mas permanece inconsciente a respeito de qual mensagem foi transferida. A fim de garantir a privacidade dos nodos em uma rede, e tentar impedir a revelação de informações relevantes através de pacotes de roteamento, protocolos de roteamento anônimo foram propostos. A primeira forma de *transferência inconsciente* foi introduzida em 1981 por **Michael O. Rabin** (1931), um matemático israelense e cientista da computação que recebeu o Prêmio Turing. Nesta forma, o remetente envia uma mensagem ao receptor com probabilidade  $1/2$ , enquanto o remetente permanece indiferente se o receptor recebeu ou não a mensagem. Ver em *Oblivious Transfer* em <[https://en.wikipedia.org/wiki/Oblivious\\_transfer](https://en.wikipedia.org/wiki/Oblivious_transfer)>. Trabalhos posteriores revelaram que a *transferência inconsciente* é um problema fundamental e importante na criptografia. É considerado um dos problemas críticos no campo, devido à importância dos aplicativos que podem ser construídos com base em OT. Em particular, é bem adequado para uma *secure multi-party computation*, também conhecida por *privacy preserving computation*, a qual pode ser estudada no campo dos anonymous protocols (protocolos com anonimato). O leitor pode entender este tema em (TAMASHIRO, 2007).
- *Superdense coding* (codificação superdensa) - o primeiro e mais básico exemplo de comunicação assistida por emaranhamento quântico) (BENNETT; WIESNER, 1992).

A ideia de utilizar a mecânica quântica de forma parecida a utilizada hoje em criptografia quântica, foi apresentada em 1970 por **Stephen Wiesner**, quando estudante de pós-graduação da *University of de Columbia*. Ele demonstrou a possibilidade teórica de se fazer "dinheiro quântico", impossível de ser falsificado graças a um sistema de armazenamento quântico de *qubits*.

Longe de ser uma ideia prática, a ideia era revolucionária. Anos mais tarde **Bennett** e **Brassard** inspiraram-se nessa ideia de "dinheiro quântico" para criar o protocolo



Figura 191 – Stephen Wiesner - Aos 28 anos, a ideia em 1970 que norteou a criptografia quântica por Charles Bennett.

Fonte: <<https://www.mpiwg-berlin.mpg.de/research/projects/origin-and-development-quantum-cryptography>> (mpiwg-berlin.mpg.de)

BB84. Contudo, o mais interessante dessa história consiste em a ideia de **Wiesner** ter sido absolutamente ignorada no seu tempo. O seu orientador pediu-lhe que abandonasse a ideia e voltasse ao "trabalho", mostrando total desinteresse por ela.

Conta **Wiesner** - "*Não obtive nenhum apoio do meu orientador de tese - ele não mostrou o mínimo interesse pela minha ideia. Mostrei-a para outras várias pessoas e todas fizeram uma cara de estranheza e voltaram ao que já estavam fazendo naquela hora*".

Apesar disso, **Wiesner** submeteu a sua ideia para ser publicada numa revista científica. O artigo foi recusado. Submeteu-o a outras três revistas, e outras três vezes ele foi recusado. Embora tenha sido rejeitado por várias revistas científicas, o trabalho de **Stephen Wiesner** permaneceu inédito por mais de uma década, até 1983, mas circulou bastante em forma de manuscrito para estimular o surgimento da ciência da informação quântica nas décadas de 1980 e 1990. A partir de 2013, **Wiesner** resolveu trabalhar (por opção) como operário de construção em Jerusalém ([SCOTT, 2013](#)). Atualmente tem 77 anos.

Desiludido, mas consciente do grande interesse de **Bennett** por assuntos mais amplos, **Wiesner** enviou o seu rejeitado artigo a ele. **Bennett** ficou imediatamente fascinado pela ideia, mostrando-a para **Brassard**. Alguns anos depois, os dois juntos, inspirados na ideia de utilizar a mecânica quântica como proposto por **Wiesner**, inventaram o que hoje em dia é reconhecido no campo da criptografia quântica. O "dinheiro quântico" é um projeto proposto de notas de banco, tornando-as impossíveis de forjar, usando a física quântica. A ideia influenciou o desenvolvimento de protocolos de distribuição quântica de chaves usados na criptografia quântica.

A segunda história refere-se ao momento no qual **Bennett** e **Brassard** inventaram



o protocolo BB84. Em 1984 fazia já algum tempo que ambos vinham tentando achar uma solução para o problema da distribuição de chaves, num cenário futurístico onde a computação quântica inviabilizara os atuais métodos de criptografia de chave pública. Um dia, quando estavam esperando o trem que levaria **Brassard** para casa, em Montreal, desde os laboratórios *Thomas. J. Watson*, da IBM, onde **Bennett** trabalhava, a solução para o problema surgiu. Esperando o trem na estação *Croton Harmon*, conversando descontraída e informalmente, eles tiveram a brilhante ideia que levou ao protocolo BB84. Como afirma **Simon Singh** em seu livro *The Code Book* (SINGH, 2000), se o trem tivesse chegado apenas alguns minutos antes eles teriam se despedido sem fazer nenhum progresso no problema da distribuição de chaves (RIGOLIN; RIEZNIK, 2005).

## 12.6 A primeira ideia de um sistema de criptografia quântico

A partir da ideia inicial de **Stephen Wiener**, **Charles Bennett**, cientista de computação da IBM em Nova York, na década de 1980, em conjunto com um colega, **Gilles Brassard**, conseguiu idealizar um primeiro sistema de criptografia quântico prático. Tempos seguintes, os avanços tecnológicos permitiram pôr em prática protótipos de sistemas criptográficos que parecem ser absolutamente invioláveis.

**Charles Henry Bennett** (1943-), nascido em New York, é um físico, criptógrafo e cientista da computação estadunidense. É um dos descobridores do *teletransporte quântico*. Ele obteve o Bacharelado em química pela Brandeis University em 1964, e o Doutorado em Harvard em 1970 por estudos de dinâmica molecular (simulação computacional do movimento molecular) com **David Turnbull** e **Berni Alder**, seus orientadores acadêmicos. Nos dois anos seguintes, ele continuou esta pesquisa com o físico indiano **Aneesur Rahman** (1927-1987) no *Argonne National Laboratory*.



Figura 192 – Charles Henry Bennett é um físico, criptógrafo e cientista da computação estadunidense. É um dos descobridores do teletransporte quântico.

Fonte: <[https://pt.wikipedia.org/wiki/Charles\\_Henry\\_Bennett](https://pt.wikipedia.org/wiki/Charles_Henry_Bennett)>, <<http://john.kangry.com/>>

*Teletransporte quântico* é uma tecnologia que permite o teletransporte de informação <[https://pt.wikipedia.org/wiki/Teletransporte\\_quântico](https://pt.wikipedia.org/wiki/Teletransporte_quântico)>, como o *spin* <<https://pt.wikipedia.org/wiki/Spin>> ou a *polarização* (não existe transporte de energia ou de matéria) por meios exclusivamente quânticos, que independem de meios de transmissão. A largura de banda para o teletransporte quântico dobrou em 2015. Uma técnica chinesa de transferências informações sobre uma partícula de modo que uma outra partícula toma duas, em vez de apenas uma, das propriedades quânticas da partícula inicial <<https://www.sciencenews.org/article/physicists-double-their-teleportation-power>>.

*Teletransporte* de informações, proposto pela primeira vez em 1993 por físicos teóricos que trabalhavam para a empresa IBM, utiliza um efeito da mecânica quântica chamado de *emaranhamento/entrelaçamento quântico*, pelo qual partículas subatômicas que passam por processos quânticos mantêm um tipo de associação intrínseca mesmo depois de separadas, à semelhança do fenômeno de ressonância, mas teoricamente independente da distância. O exemplo mais citado é o de duas partículas criadas conjuntamente que assumem *spins* opostos, e ao se determinar o *spin* de uma, o *spin* da outra fica instantaneamente determinado, mesmo que elas estejam separadas. A tecnologia tenta usar esse efeito para telecomunicações ou armazenamento de informação num possível computador quântico.

## 12.7 Entropia da Informação

O conceito de entropia pode ser explicado a diversas áreas do conhecimento. Neste contexto, o conceito de entropia se relaciona com o de *entropia da informação*.

*Informação* é um termo que vem sendo usado, a partir da década de 1950, por diferentes autores, significando mensagens, notícias, novidades, dados, conhecimento, literatura, símbolos, signos (signo linguístico é um elemento representativo que apresenta dois aspectos: o significado e o significante; ao escutar a palavra cavalo, reconhecemos a sequência de sons que formam essa palavra) e, até mesmo, sugestões.

A quantidade de informação de uma mensagem é calculada, na Teoria da Informação, como sendo o menor número de bits, unidade de informação introduzida por **Shannon** (vide abaixo), necessários para conter todos os valores ou significados desta mensagem. Assim, por exemplo, para codificar uma das 26 letras do nosso alfabeto, bastam 4 bits, pois eles podem armazenar  $2^4 = 16$  valores diferentes, enquanto que 8 bits (1 byte) conseguem armazenar os 256 caracteres (28) da codificação ISO 8859-1 de caracteres do alfabeto latino, com seus diacríticos (um sinal gráfico que se coloca sobre, sob ou através de uma letra para alterar a sua realização fonética, isto é, o seu som, ou para marcar qualquer outra característica linguística).

Em 1948, o matemático norte-americano **Claude Elwood Shannon** (1916-2001) introduziu o conceito de *entropia da informação*, a qual *quantifica o grau de incerteza de uma informação*. Segundo ele, sempre que uma mensagem passa por um canal de comunicação, ela sofre perturbações e chega com ruídos ao receptor. **Shannon** enxergou aí uma analogia entre os processos onde há perda de informação e os processos que ganham entropia.

Segundo **Norbert Wiener** (1894-1964) um matemático estadunidense, conhecido como o fundador da cibernética.



Figura 193 – Claude Shannon em 1963 - Um matemático, engenheiro eletrônico e criptógrafo estadunidense, conhecido como o pai da "teoria da informação".

Fonte: <[https://pt.wikipedia.org/wiki/Claude\\_Shannon](https://pt.wikipedia.org/wiki/Claude_Shannon)> ,

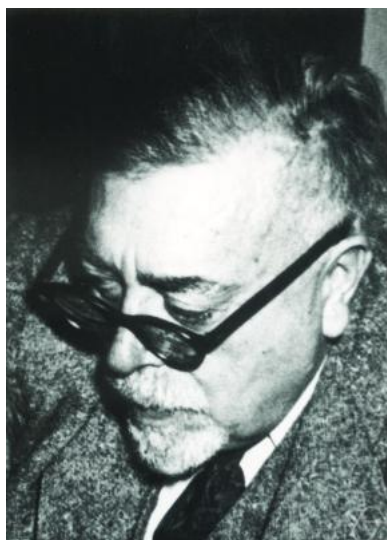


Figura 194 – Norbert Wiener - Sobre a entropia da informação: o grau de organização ou desorganização em um sistema de informação.

Fonte: <[https://pt.wikipedia.org/wiki/Norbert\\_Wiener](https://pt.wikipedia.org/wiki/Norbert_Wiener)> ,

*"... a soma de informação em um sistema de comunicação de informação é a medida de seu grau de organização; a entropia é a medida de seu grau de desorganização; um é o negativo do outro."*

Como um exemplo pitoresco, no processo de mistura de café com leite, inicialmente, antes de se misturarem, teremos, **no mínimo três informações**: (a) café quente; (b) leite, eventualmente gelado; (c) açúcar, à temperatura ambiente. Após a mistura, teremos apenas **uma** informação: café-com-leite-adoçado-morno.

Com isso, em termos do *conceito de informação*, a entropia negativa, pode ser aplicado para exprimir a medida da ordenação/desordenação de um sistema de comunicação de informação. Na verdade, a *entropia de informação* foi estendida às mais diversas áreas de conhecimento, tal como na Ciência da Informação, dentre outras.

## 12.8 A Criptografia quântica de Bennett

No processo proposto por **Bennett**, o emissor da mensagem, Alice, (ver a Figura 195) começa por digitalizar o texto que pretende enviar para o receptor Bob, transformando-o numa sequência de zeros e uns, a linguagem dos computadores. Ela toma, então uma chave criptográfica, que é outra sequência de zeros e uns tão longa quanto a mensagem original, e adiciona as duas fileiras de números. Transmite o resultado a Bob, que tem consigo a chave que Alice utilizou. Bob subtrai-lhe a chave e recupera a mensagem original. Para ler, terá naturalmente de transformar a sequência de zeros e uns, numa sequência de letras. Mas, isto é uma tarefa rotineira para qualquer computador.

Para este sistema ser verdadeiramente inviolável é importante que a chave seja uma sequência aleatória de zeros e uns e que seja utilizada apenas uma vez. Isso significa que esses números tem de ser gerados antecipadamente e que Alice tem de os transmitir a Bob.

E aqui começam os problemas. Se Alice e Bob nunca se encontram pessoalmente, como acontece habitualmente com parceiros no comércio eletrónico, eles têm de confiar num método de transmissão da chave. E como vão fazê-lo? De forma cifrada? Mas, para isto precisam ter acordado numa outra chave, e então o problema parece não ter solução. Em alguma altura, Alice e Bob terão de se encontrar ou confiar num mensageiro. Mas, supondo que, um intruso, Eva, que está sempre à espreita, a segurança absoluta não existe.

Entra aqui o mundo quântico pela mão de **Charles Bennett** e dos cientistas da computação. Esse mundo tem regras estranhas, impossíveis de intuir com base nas nossas vivências cotidianas. Uma delas é a *incerteza*. E essa *incerteza* não se baseia no nosso desconhecimento, é intrínseca à própria vida das partículas subatômicas.

Alice começa enviar a Bob uma sequência de partículas de luz, ou seja, uma sequência de fótons. No seu aparelho existem dois polarizadores, um orientado na vertical e outro a 45 graus, como se pode ver na Figura 195 e na Figura 198.

Para estabelecer a chave, Alice alterna os polarizadores aleatoriamente e faz, por exemplo, corresponder 0 a um fóton polarizado na vertical, e 1 a um fóton que seja polarizado a  $-45^\circ$ . Bob tem consigo outros dois polarizadores. Um orientado na horizontal e outro a  $-45^\circ$ . Ao receber cada fóton esse é passado por um dos seus polarizadores, alternando entre os dois, de forma completamente aleatória.

## 12.9 Um sistema prático de criptografia quântica

Em colaboração com **Gilles Brassard** (1955-) da Universidade de Montreal, **Bennett** desenvolveu um sistema prático de criptografia quântica, baseado no

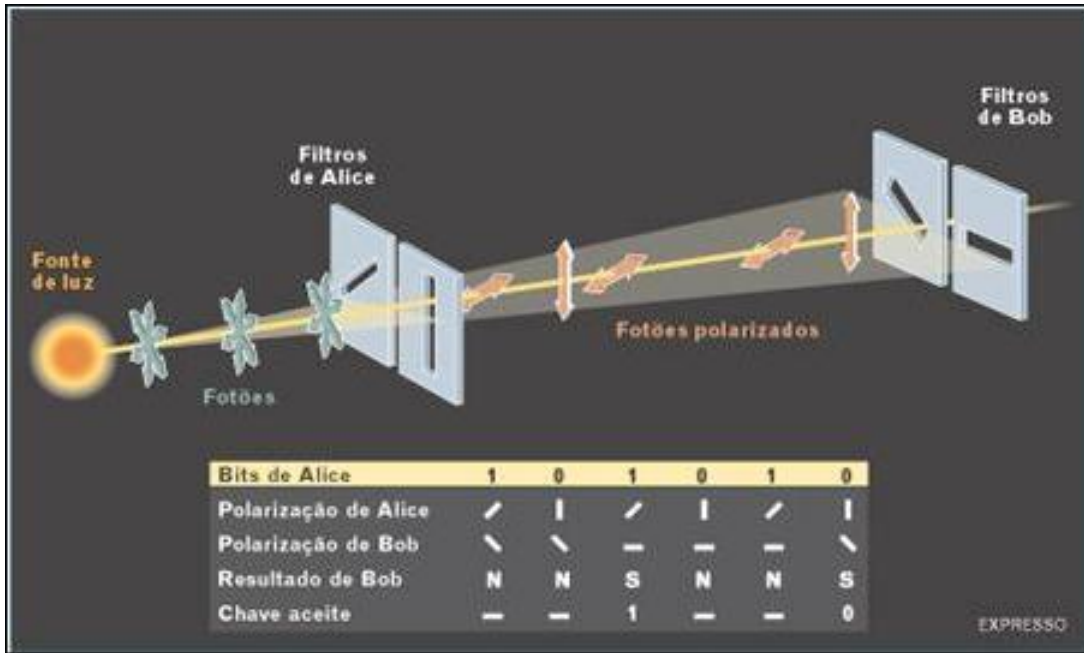


Figura 195 – Polarizações de fótons na comunicação de Alice e Bob.

Fonte: Google Images

princípio da incerteza, conhecido como BB84 (BENNETT; BRASSARD, 1984), que permite a comunicação segura entre as partes que inicialmente, não compartilham nenhuma informação secreta. Em 1989, com a ajuda de **John A. Smolin**, Bennett fez a primeira demonstração mundial do trabalho da criptografia quântica.

**Gilles Brassard** é um criptologista canadense. Estudou na Universidade de Montreal, em 1975, e obteve seu doutorado em ciência da computação pela Universidade Cornell em 1979, trabalhando no campo da criptografia com **John Hopcroft** () como seu supervisor. É um membro do corpo docente da Universidade de Montreal desde então, onde se tornou professor titular em 1988. **Brassard** é mais conhecido por seu trabalho fundamental na criptografia quântica, teletransporte quântico, entrelaçamento quântico e na simulação clássica de *entrelaçamento quântico*. Alguns destes conceitos são ainda teóricos, mas outros têm sido implementados em laboratório.

Os interesses de pesquisa de **Charles Bennett** incluem a teoria algorítmica da informação, na qual os conceitos de informação e aleatoriedade são desenvolvidos nos termos da relação input/output (entrada/saída) dos computadores universais (Máquina de Turing), e à utilização destes para definir a complexidade intrínseca ou "profundidade lógica" de um estado físico, como o tempo exigido por um computador universal para, a partir de um estado aleatório inicial, simular a evolução de um estado quântico (BENNETT, 1996).

## 12.10 O Protocolo BB84

O protocolo conhecido como BB84 (EKERT, 1991) em função de seus inventores e do ano de publicação (CLAUSER et al., 1969), foi originalmente descrito utilizando os estados de polarização dos fótons para transmitir a informação. Ao



Figura 196 – Gilles Brassard - Juntamente com Charles Bennett desenvolveu um sistema prático de criptografia quântica, baseado no princípio da incerteza, conhecido como BB84.

Fonte: <[https://pt.wikipedia.org/wiki/Gilles\\_Brassard](https://pt.wikipedia.org/wiki/Gilles_Brassard)>

trocarem entre as suas várias posições possíveis, os fótons vibram e se, num grupo de fótons, todos vibram na mesma direção, então eles estão polarizados. Utilizando filtros polarizadores é possível restringir a passagem aos fótons polarizados numa determinada direção, bloqueando os restantes. Para medir a polarização de um fóton são utilizadas bases de medida, que são compostas por duas direções que façam um ângulo reto. Por exemplo: horizontal e vertical, ou diagonal à esquerda e à direita. No entanto, qualquer dois pares de variáveis conjugadas pode ser utilizado para o protocolo.

Os estados de polarização mais utilizados são:

- Base retilínea com vertical ( $0_0$ ) e horizontal ( $90_0$ ).
- Base diagonal com os ângulos de  $45_0$  e  $135_0$ .
- Base circular com a direita e esquerda, seguindo a regra da mão direita.

Qualquer duas bases listadas acima são conjugadas uma das outra e então podem ser utilizadas para o protocolo. Nos exemplos a seguir, as bases retilínea e diagonal são utilizadas. Este é um protocolo de bases conjugadas.

O emissor (tradicionalmente conhecido como Alice) e o receptor (Bob) estão conectados por um canal de comunicação quântica, que permite a transmissão de

Base	0	1
+	↑	→
×	↗	↘

Figura 197 – Criptografia Quântica - A comunicação quântica entre Alice e Bob.

Fonte: <[https://pt.wikipedia.org/wiki/Criptografia\\_quântica](https://pt.wikipedia.org/wiki/Criptografia_quântica)>

estados quânticos, por exemplo, fibra ótica, que permite a transmissão de fótons. Eles também se comunicam via um canal clássico público, como telefone ou internet. Nenhum desses canais precisa ser seguro; o protocolo é escrito assumindo-se que um espião (chamado de Eva) pode interferir de qualquer maneira com qualquer um dos canais.

O primeiro passo no protocolo BB84 é a transmissão quântica. Alice cria um bit aleatório (0 ou 1) e depois aleatoriamente seleciona uma das duas bases (retilínea ou diagonal nesse caso) para transmitir o fóton. Ela então prepara a polarização do fóton dependendo da base e do valor do bit. Alice então transmite um único fóton no estado especificado para o Bob, usando o canal quântico. Esse processo é repetido desde a criação do bit aleatório, com Alice anotando o valor do bit, a base utilizada e a hora que o fóton foi enviado.

A mecânica quântica diz que **não existe medida possível que possa distinguir entre 4 estados diferentes de polarização**, visto que **eles não são todos ortogonais. A única medida possível é entre qualquer dois estados ortogonais (ou base)**. Se Bob, por exemplo, medir na base retilínea, ele terá como resultado ou horizontal ou vertical. Se o fóton foi criado inicialmente em uma dessas polarizações, então ele medirá o estado correto; mas se o fóton tiver sido criado na base diagonal, então a medida na base retilínea tornará o fóton polarizado vertical ou horizontalmente de maneira aleatória e a informação sobre sua polarização inicial será perdida.

Como Bob não sabe em que base os fótons foram criptografados, tudo que ele pode fazer é selecionar aleatoriamente uma base para cada medida. Ele faz isso para cada fóton recebido e anota o tempo, a base utilizada e o resultado da medida. Depois de Bob ter medido todos os fótons, ele se comunica com a Alice via um canal clássico público. Alice então informa a Bob a base que foi utilizada para preparar cada fóton e Bob informa as bases que ele utilizou para medi-los. Eles então descartam os valores medidos em que Bob usou a base errada. Segundo este método, as probabilidades de Bob utilizar os filtros corretos é de 50% (uma base de medida correta em duas possíveis). Logo, para se obter uma palavra binária de  $n$  bits, é necessário enviar o dobro de fótons.

Quando alguém (Bob ou Eva) ler a mensagem enviada, a mensagem é automaticamente alterada de forma irreversível, pois como já vimos, a medição da polarização dos fótons tem essa inevitável consequência. Assim, tudo o que quem interceptar as comunicações pode fazer é testar um conjunto de bases, ficando sem saber em quais acertou. Mesmo que Eva também intercepte as comunicações realizadas no canal público, ela ficará sem saber o valor da chave final. Isto porque através desta

Bit aleatório de Alice	0	1	1	0	1	0	0	1
Base aleatória selecionada por Alice	+	+	×	+	×	×	×	+
Polarização do fóton enviado por Alice	↑	→	↘	↑	↘	↗	↗	→
Base de medida aleatória selecionada por Bob	+	×	×	×	+	×	+	+
Fóton polarizado medido por Bob	↑	↗	↘	↗	→	↗	→	→
DISCUSSÃO PÚBLICA SOBRE AS BASES								
Chave Secreta partilhada	0		1			0		1

Figura 198 – Criptografia Quântica BB84 - A comunicação quântica entre Alice e Bob.

Fonte: <[https://pt.wikipedia.org/wiki/Criptografia\\_quântica](https://pt.wikipedia.org/wiki/Criptografia_quântica)>

comunicação, apesar de se saber quais os fótons que contribuem para a chave não se sabe com que valor. Falaremos mais a seguir sobre algumas técnicas de espionagem.

### Criptografia quântica

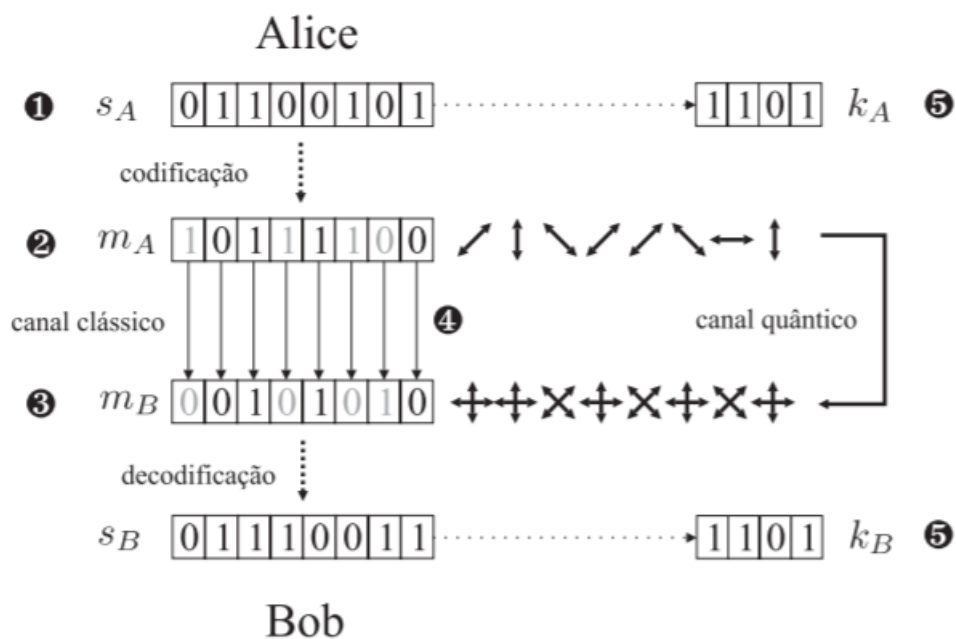


Figura 199 – Criptografia Quântica BB84 - Passos de execução do protocolo BB84 no caso ideal.

Fonte: <[https://www.teses.usp.br/teses/disponiveis/3/3141/tde-25092008-101016/publico/dissert\\_carlostcosta.pdf](https://www.teses.usp.br/teses/disponiveis/3/3141/tde-25092008-101016/publico/dissert_carlostcosta.pdf)>

Para testar se Eva estava interceptando a mensagem, Alice e Bob comparam um certo número de fótons na sua chave secreta. Se a terceira parte tiver conseguido alguma informação sobre a polarização dos fótons, isto irá introduzir erros nas medidas de Bob. Se mais de  $p$  bits forem diferentes, eles apagam essa chave e tentam novamente, possivelmente com um canal quântico diferente, uma vez que a segurança da chave não pode ser garantida. O número  $p$  é escolhido de forma que o número de bits conhecidos por Eva seja menor que ele, a amplificação da privacidade pode ser utilizada para reduzir o conhecimento de Eva sobre a chave para um valor arbitrariamente



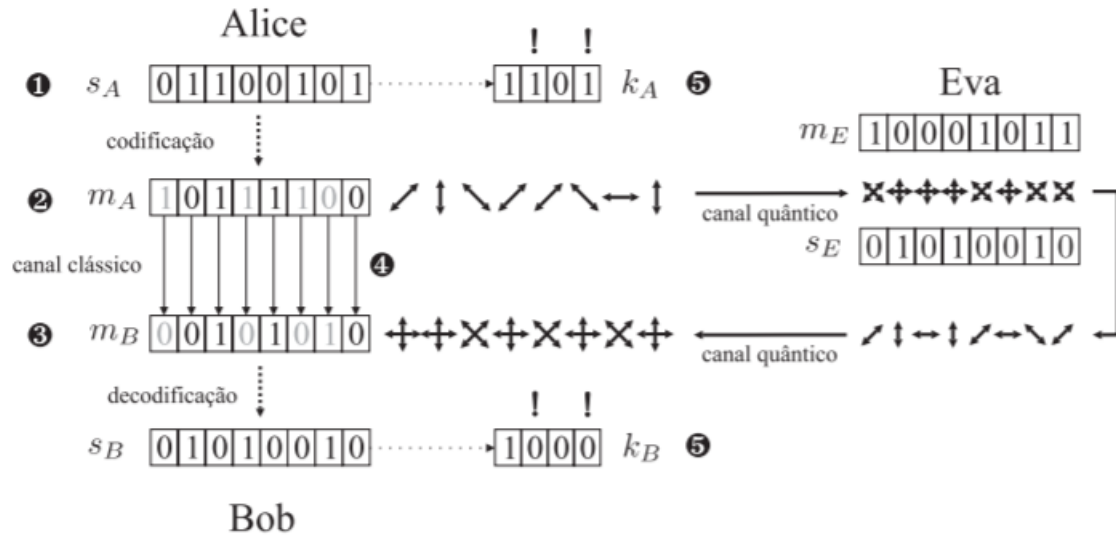


Figura 200 – Criptografia Quântica BB84 - Passos de execução do protocolo BB84 na presença de Eva.

Fonte: <[https://www.teses.usp.br/teses/disponiveis/3/3141/tde-25092008-101016/publico/dissert\\_carloscosta.pdf](https://www.teses.usp.br/teses/disponiveis/3/3141/tde-25092008-101016/publico/dissert_carloscosta.pdf)>

pequeno, através da redução do tamanho da chave.

Este protocolo é usado em todos os sistemas bem-sucedidos de criptografia quântica instalados até hoje e, mais ainda, ele é o único oferecido por duas companhias especializadas em segurança de transmissão de dados. Assim, mesmo sendo o primeiro protocolo proposto na literatura, ele ainda é, apesar das muitas alternativas de criptografia quântica apresentadas, *a posteriori*, aquele de maior importância prática e comercial (RIGOLIN; RIEZNIK, 2005).

Em (BENNETT; BRASSARD, 1984) (BENNETT; BRASSARD, 1984) foi apresentado, pela primeira vez, a ideia de que a mecânica quântica podia ser utilizada para alcançar uma das principais metas da criptografia, isto é, a **distribuição segura de uma chave criptográfica** (sequência de números aleatórios) entre duas partes (Alice e Bob) que inicialmente não compartilham nenhuma informação secreta. Para isso, Alice e Bob devem dispor não só de um canal quântico, mas também de algum canal clássico de comunicação. Este último pode ser monitorado passiva mas não ativamente por um agente externo (Eva). Por meio dessa chave, Alice e Bob podem com absoluta certeza se comunicar com segurança. A garantia da distribuição segura de chaves por meio da criptografia quântica, se sustenta na validade da MQ tal qual a conhecemos. Em contraste, a criptografia de chave pública é considerada segura devido a um suposto grau de complexidade matemática inerente ao algoritmo de decodificação necessário para recuperar a mensagem criptografada se não conhecemos a chave privada. No entanto, esse resultado nunca foi matematicamente provado e não há nada que impeça a criação de um algoritmo que possa facilmente decodificar, por meio de computadores convencionais, mensagens secretas oriundas de protocolos de chaves públicas. Pior ainda, a segurança da criptografia de chave pública tradicional desabaria perante o aparecimento de computadores quânticos, o que não aconteceria com sistemas de distribuição de chaves por criptografia quântica

(RIGOLIN; RIEZNIK, 2005).

Este protocolo utiliza-se de sistemas quânticos de criptografia quântica de dois níveis. Assim, os estados  $|0\rangle$  e  $|1\rangle$  representam fótons linearmente polarizados em direções ortogonais. Por exemplo, os estados  $|0\rangle$  e  $|1\rangle$  podem representar fótons que se propagam na direção  $z$  com campos elétricos oscilando no plano  $xy$ . As direções de polarização são representadas por vetores unitários. Usando coordenadas esféricas, de acordo com a notação definida na Figura 201, precisamos de dois parâmetros (ângulos) para especificar uma direção de polarização. Na Figura 201, o ângulo polar  $\theta$  varia de  $0$  a  $\pi$  e o ângulo  $\phi$  de  $0$  a  $2\pi$ . Aqui, o vetor  $r$ , de módulo  $r$ , tem projeção no plano  $xy$  dada por  $\rho = r \cdot \sin\theta$ . As coordenadas cartesianas se relacionam com as coordenadas esféricas pela seguinte equação:

$$\hat{r} = x\hat{x} + y\hat{y} + z\hat{z} = r \cdot \sin\theta \cdot \cos\phi\hat{x} + r \cdot \sin\theta \cdot \sin\phi\hat{y} + r \cdot \cos\theta\hat{z}.$$

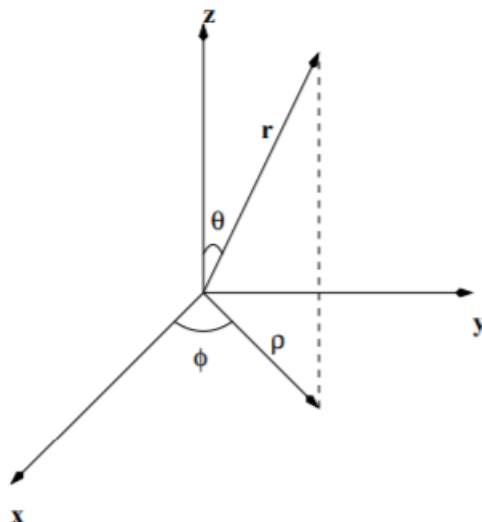


Figura 201 – Coordenadas esféricas - Indicando a direção das polarizações.

Fonte: (RIGOLIN; RIEZNIK, 2005)

Alice e Bob devem primeiramente escolher duas bases que serão utilizadas para a transmissão e recepção dos fótons. Cada base é composta por dois estados ortogonais de polarização, como está mostrado na Figura 202. Eles podem escolher, por exemplo, polarizações contidas no plano  $xy$  ( $\theta = \pi/2$ ). Tomando  $\phi = 0$  e  $\phi = \pi/2$ , definimos as direções de polarização de uma das bases (base A). Usando  $\theta = \pi/4$  e  $\phi = 3\pi/4$  obtemos a outra (base B).

O estado de polarização de qualquer fóton pode ser representado como *uma combinação linear de dois estados ortogonais de polarização*. Dessa forma, por meio dos estados que formam a base A ou a base B, podemos representar qualquer estado de polarização de um fóton. Alice e Bob também devem combinar previamente quais estados ortogonais de cada uma das bases representam o bit 0 e o bit 1. Isso pode ser feito via um canal tradicional (clássico) de comunicação.

No exemplo, utilizamos os fótons polarizados na direção  $\phi = 0$  ou  $\phi = \pi/4$  para

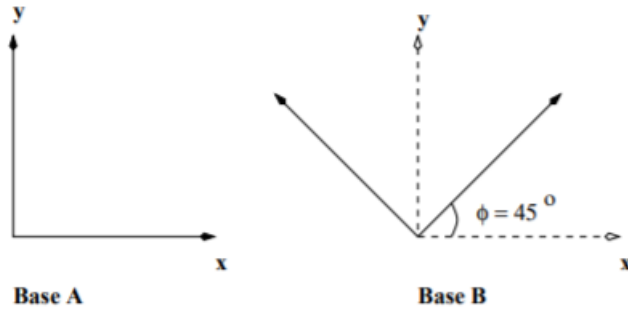


Figura 202 – Representação das bases A e B. O eixo z não está desenhado pois temos polarizações pertencentes ao plano xy.

Fonte: (RIGOLIN; RIEZNIK, 2005)

representar o bit 0 ( $|0\rangle_A$  e  $|0\rangle_B$ ) e aqueles com polarização na direção  $\phi = \pi/2$  ou  $\phi = 3\pi/4$  representando o bit 1 ( $|1\rangle_A$  e  $|1\rangle_B$ ). Nesta notação, o subíndice em cada ket indica se temos fótons polarizados nos autoestados da base A ou B. Note que  $|0\rangle_B = (1/\sqrt{2})(|0\rangle_A + |1\rangle_A)$  e  $|1\rangle_B = (1/\sqrt{2})(|0\rangle_A - |1\rangle_A)$ .

Alice, para transmitir a chave, procede da seguinte forma. Primeiro ela escolhe qual sequência aleatória de bits que enviará a Bob (vamos usar, por exemplo, 001111...). Depois, qual a base utilizada para transmitir cada bit. Ela pode transmitir os dois primeiros bits utilizando-se da Base A, os três bits seguintes utilizando-se da Base B, o bit seguinte utilizando-se novamente da Base A, e assim por diante. Dessa forma, ela estaria enviando a Bob uma sequência de fótons representados pelos seguintes kets:  $|0\rangle_A$ ,  $|0\rangle_A$ ,  $|1\rangle_B$ ,  $|1\rangle_B$ ,  $|1\rangle_B$ ,  $|1\rangle_A$ , etc. Bob, por sua vez, deve escolher apenas qual base ele irá utilizar para detectar cada fóton. Ele oscila entre as bases A e B aleatoriamente. Após a transmissão e detecção dos fótons, Alice e Bob revelam publicamente quais bases utilizaram para enviar e detectar cada fóton, respectivamente. Mas Alice não revela se enviou 0s ou 1s e Bob não revela o resultado de suas medidas. Apenas as bases utilizadas (base A ou base B) são publicamente reveladas. A seguir, eles consideram apenas os resultados nos quais ambos utilizaram a mesma base, descartando todos os demais. Agora eles revelam publicamente uma parte destes resultados (metade, ou um terço, por exemplo). Se Eva não monitorou a transmissão, os resultados revelados por Bob e Alice devem coincidir; mas se ela a monitorou, a probabilidade de que todos os dados públicos coincidam é praticamente nula (provamos isso um pouco mais à frente). Se os dados revelados publicamente coincidirem, isso será uma prova de que Eva não monitorou a transmissão e eles podem usar o restante dos dados como a chave. Por restante dos dados entendemos aqueles nos quais ambos usaram a mesma base para enviar e medir os fótons. E aqui termina o protocolo. Se Eva monitorou os dados, a parte da informação revelada publicamente por Alice e Bob não irá coincidir ou, mais rigorosamente, a probabilidade de que elas coincidam é praticamente nula.

A prova deste fato é como segue. Para simplificar a demonstração e sem perda de generalidade, supomos que Alice, Bob e Eva utilizam metade das vezes, a Base A e metade das vezes a Base B, Alice para transmitir e Eva e Bob para detectar os fótons. Se Alice e Bob utilizam a mesma base, a probabilidade de Eva usar a mesma base vale 0.5 (se Alice e Bob utilizaram a Base A, por exemplo, a proba-

bilidade de Eva também ter utilizado essa base é 0.5). Agora, se Eva utiliza para monitorar os fótons a outra base, a probabilidade de Bob medir corretamente o valor do bit transmitido é de apenas 0.5 e não 1, como deveria ser se não tivéssemos um espião ou se Eva tivesse optado pela base correta. Formalmente, suponhamos que Alice enviou o fóton representando o bit 1, na Base A ( $|1\rangle_A$ ) e Bob corretamente mediu na base A, porém Eva mediu o fóton, antes de ele chegar a Bob, na base B. Procedendo dessa forma, Eva terá colapsado o estado de polarização dos fótons em um dos autovetores da base por ela utilizada, i.e.,  $|0\rangle_B = (1/\sqrt{2})(|0\rangle_A + |1\rangle_A)$  ou  $|1\rangle_B = (1/\sqrt{2})(|0\rangle_A - |1\rangle_A)$ . Assim, quando Bob realizar sua medida, a chance de ele medir,  $|1\rangle_A$  é de apenas  $(1/2\sqrt{2}) = 0.5$ , independente do resultado obtido por Eva. O fato de Eva escolher a base errada implica, para um evento, uma probabilidade igual a 0.5 de Bob detectar o valor correto para o bit transmitido por Alice. Para uma chave muito grande, a probabilidade de Bob detectar todos os bits corretamente, com Eva interferindo, tende a zero ou, mais rigorosamente, a  $(0.5)^N$ , onde  $N$  é o número de vezes que Eva usou a base errada.

Vale a pena lembrar que **estados quânticos arbitrários não podem ser clonados**. Isso foi demonstrado independentemente por **Wootters** e **Zureck** (**WOOTTERS; ZUREK, 1982**) e por **Dieks** (**DIEKS, 1982**). Isso garante que Eva não pode simplesmente duplicar o estado quântico dos fótons enviados por Alice, medir um deles e enviar a Bob o outro. Isso possibilitaria a Eva detectar a polarização correta dos fótons transmitidos por Alice sem ser descoberta, tornando o protocolo BB84 inseguro.

Para melhor entender todas as etapas do protocolo, a Figura 203 simula um exemplo de transmissão de *chave quântica*. Consideramos uma situação bem geral, na qual alguns fótons podem se perder durante a transmissão, de forma que Bob não os recebe.

Tabela 1 - As cinco primeiras linhas correspondem à transmissão quântica. As outras cinco, à discussão pública entre Alice e Bob. A última representa a chave compartilhada por eles.

Seqüência de bits de Alice	0	1	1	0	1	1	0	0	1	0	1	1
Bases escolhidas por Alice	B	A	B	A	A	A	A	A	B	B	A	B
Fótons enviados por Alice	$ 0\rangle_B$	$ 1\rangle_A$	$ 1\rangle_B$	$ 0\rangle_A$	$ 1\rangle_A$	$ 1\rangle_A$	$ 0\rangle_A$	$ 0\rangle_A$	$ 1\rangle_B$	$ 0\rangle_B$	$ 1\rangle_A$	$ 1\rangle_B$
Bases escolhidas por Bob	A	B	B	A	A	B	B	A	B	A	B	B
Bits recebidos por Bob	1		1		1	0	0	0		1	1	1
Bob informa fótons detectados	A		B		A	B	B	A		A	B	B
Alice informa bases corretas			OK		OK			OK				OK
Informação compartilhada			1		1			0				1
Bob revela alguns bits da chave					1							
Alice confirma estes bits					OK							
Restante de bits é a chave			1					0				1

Figura 203 – As cinco primeiras linhas correspondem à transmissão quântica. As outras cinco, à discussão pública entre Alice e Bob. A última linha representa a chave compartilhada por eles.

Fonte: (**RIGOLIN; RIEZNIK, 2005**)

**John A. Smolin** (1967-), nascido em New York, é um físico americano e membro da *American Physical Society* no *Thomas J. Watson Research Center* da IBM. **Smolin** é mais conhecido por seu trabalho na teoria da informação quântica, onde, com colaboradores, apresentou várias técnicas importantes (**BENNETT, 1996**) incluindo a *destilação de emaranhamento*, a *correção de erros quânticos* e a *transmissão fiel*

da *informação quântica* através de canais quânticos ruidosos, bem como para a transmissão assistida em paralisação de informações clássicas. Ele ajudou a elucidar as relações complexas entre as capacidades clássicas e quânticas de vários canais (DIVINCENZO; SHOR; SMOLIN, 1999), bem como fenômenos como o *data hiding* e o *data unlocking* que não possuem análises na teoria da informação clássica. Juntamente com **Charles H. Bennett**, ele construiu a primeira demonstração de criptografia quântica em 1989 (BENNETT et al., 1992), conduzida por software escrito por **François Bessette**, **Gilles Brassard** e **Louis Salvail** e implementando o protocolo de distribuição de chaves quânticas BB84. **Smolin** cunhou o termo "*Church of the Larger Hilbert Space*" para descrever o hábito de considerar cada estado misto de um sistema quântico como um estado puro emaranhado de um sistema maior e toda evolução irreversível como uma evolução reversível (unitária) de um sistema maior (BENNETT et al., 1992).



Figura 204 – John A. Smolin - Juntamente com Charles H. Bennett, construiu a primeira demonstração de criptografia quântica em 1989.

Fonte: <[https://pt.wikipedia.org/wiki/John\\_A.\\_Smolin](https://pt.wikipedia.org/wiki/John_A._Smolin)>, <<http://john.kangry.com/>>

**William Kent Wootters** (1951-) é um físico teórico americano e um dos fundadores do campo da teoria da informação quântica. Em um artigo conjunto com **Wojciech H. Zurek**, ele provou o *teorema da não-clonagem*, também descoberto independentemente por **Dennis Dieks**. Ele é conhecido por suas contribuições para a teoria do *emaranhamento quântico*, incluindo medidas quantitativas do mesmo, comunicação assistida por *emaranhamento*, notavelmente o *teletransporte quântico*, descoberto por **Wootters**, **Bennett** e **Brassard**, em 1993. O termo *qubit*, denotando a unidade básica de informação quântica, originou-se de uma conversa entre **Wootters** e **Benjamin Schumacher** em 1992.

**Benjamin Schumacher** é um físico teórico americano, trabalhando principalmente no campo da teoria quântica da informação. Ele descobriu uma maneira de interpretar estados quânticos como informação. Ele criou uma maneira de compactar as informações em um estado e armazenar as informações em um número menor de estados. Isto é agora conhecido como compressão de **Schumacher**. Seu trabalho é o análogo quântico do teorema de codificação sem ruído de **Shannon** e ajudou a iniciar o campo conhecido como *teoria da informação quântica*. É também creditado



Figura 205 – William Wootters - Teoria do emaranhamento quântico e a descoberta do teletransporte quântico.

Fonte: <[https://en.wikipedia.org/wiki/William\\_Wootters](https://en.wikipedia.org/wiki/William_Wootters)>

a **Schumacher** a invenção do termo *qubit* junto com **William Wootters**, o qual é para a computação quântica o que o *bit* é para a computação clássica.



Figura 206 – Benjamin Schumacher - Descobriu uma maneira de interpretar estados quânticos como informação.

Fonte: <[https://en.wikipedia.org/wiki/Benjamin\\_Schumacher](https://en.wikipedia.org/wiki/Benjamin_Schumacher)>

De 1995 a 1997, trabalhando com **Smolin**, **William Wootters** e **David P. DiVincenzo** e outros colaboradores, **Bennett** apresentou várias técnicas para a transmissão fiel da informação clássica e quântica através de canais ruidosos. Trabalhos recentes

realizados por **Bennett** na IBM constituem uma revisão da base física da informação e a aplicação da física quântica para problemas de fluxo de informações. Sua obra teve um papel importante no desenvolvimento de uma interligação entre a física e a informação. Um dos sistemas criptográficos, que é a base do processo proposto por **Charles Bennett** e seus colaboradores, utiliza uma chave decodificação aleatória que é tão longa quanto a mensagem sendo criptografada.

**David P. DiVincenzo** (1959-) é um físico teórico americano. É diretor do *Institute of Theoretical Nanoelectronics* no *Peter Grünberg Institute* em Jülich, e professor do *Institute for Quantum Information at RWTH Aachen University*. Com **Daniel Loss** (na University of Basel), ele propôs o computador quântico **Loss-DiVincenzo** em 1997, o qual usaria *spins* de elétrons em pontos quânticos como *qubits*.



Figura 207 – David DiVincenzo - o computador quântico baseado em spins de eletrons em 1997.

Fonte: <[https://en.wikipedia.org/wiki/David\\_DiVincenzo](https://en.wikipedia.org/wiki/David_DiVincenzo)>

**Daniel Loss** (1958-) é um físico teórico suíço e professor de Física da Matéria Condensada Teórica da Universidade de Basel e RIKEN (Um grande instituto no Japão fundado em 1917). Com **David P. DiVincenzo** (da IBM Research), ele propôs o computador quântico Loss-DiVincenzo em 1997, o qual usaria *spins* de elétrons em pontos quânticos como *qubits*.

## 12.11 O Protocolo E91

O protocolo de (**Artur Ekert** (1991) ([BENNETT; WIESNER, 1992](#)) usa pares de fótons emaranhados. Eles podem ser criados por Alice, por Bob, ou por alguma fonte separada de ambos. Os fótons são distribuídos de forma que Alice e Bob tenham um fóton de cada par. O protocolo se baseia em duas propriedades do emaranhamento quântico. Primeiro, os estados emaranhados estão perfeitamente correlacionados, de forma que, se Alice e Bob medirem se suas partículas tem polarização vertical e horizontal, eles sempre obterão a mesma resposta, com 100% de probabilidade. O mesmo é verdade se os dois medirem qualquer outro par de polarizações complementares (ortogonais). No entanto, os resultados particulares são completamente aleatórios; é impossível para Alice prever se ela (ou Bob) obterão polarização vertical ou horizontal. Segundo, qualquer tentativa de espionagem por



Figura 208 – Daniel Loss - O computador quântico Loss-DiVincenzo em 1997, baseado em spins de eletrons.

Fonte: <[https://en.wikipedia.org/wiki/Daniel\\_Loss](https://en.wikipedia.org/wiki/Daniel_Loss)>

parte de Eva irá destruir as correlações de forma que Alice e Bob poderão detectar sua presença. O leitor pode encontrar uma explicação detalhada em (RIGOLIN; RIEZNIK, 2005).

## 12.12 Protocolo B92

Em (BENNETT; BRASSARD, 1984) é demonstrada a possibilidade de se realizar a criptografia quântica utilizando apenas dois estados quânticos não-ortogonais (no protocolo BB84 (BENNETT; BRASSARD, 1984) (BENNETT; BRASSARD, 1984) tínhamos quatro estados). Sua importância é mais conceitual do que prática, pois esta proposta é difícil de ser implementada com as tecnologias atuais. A motivação que levou **Bennett** a propor este protocolo é declarada no início de seu artigo: Em (BENNETT; WIESNER, 1992) a segurança dos sistemas de distribuição de chaves que não se utilizam de emaranhamento (BB84 é um exemplo) advém do fato de que qualquer medida que não perturbe nenhum dos dois estados não-ortogonais também não fornece nenhuma informação que permita distinguir entre esses dois estados. Isto naturalmente sugere a possibilidade de que a distribuição de chaves possa ser realizada utilizando apenas dois estados não-ortogonais, como explicado em (RIGOLIN; RIEZNIK, 2005).

O protocolo B92 é muito semelhante ao anterior. Alice (A) e Bob (B) geram sequências aleatórias de bits cada um. Alice codifica os bits 0 e 1, respectivamente, nas polarizações vertical e diagonal  $+45^\circ$ . Bob decodifica, respectivamente, em diagonal  $-45^\circ$  e horizontal. Alice envia os fótons para Bob e Bob prepara o decodificador conforme a sua sequência aleatória de bits. Observe, primeiramente, que se Alice e Bob gerarem bits diferentes, as polarizações são ortogonais, de forma que há 0% de probabilidade de Bob detectar o bit. No entanto, se os bits forem iguais, a probabilidade de acerto é de 50%. Isso gera uma eficiência total de 25%. No final da comunicação, Bob anuncia as posições dos bits que ele detectou, que passarão a formar a chave (HUGHES; WILLIAMS, 2000).

Na Figura 209 as cols. 1 e 2: Sequências aleatórias geradas por A (Alice) e B (Bob); col. 3: Polarização dos fótons enviados por A (Alice); col. 4: Polarização que B



A	B	A	B	resultado	chave
0	1	↓	↔	não detecta	0 1
0	1	↓	↔	não detecta	
1	1	↗	↔	não detecta	
0	0	↓	↘	detecta	
1	1	↗	↔	detecta	
1	0	↗	↘	não detecta	
0	0	↓	↘	não detecta	
1	0	↗	↘	não detecta	

Figura 209 – Ilustração do protocolo B92.

Fonte: <[https://www.gta.ufrj.br/grad/11\\_1/quantica/trabalho003.html](https://www.gta.ufrj.br/grad/11_1/quantica/trabalho003.html)>

(Bob) prepara-se para medir; col. 5: Polarizações ortogonais ao detector têm 0% de probabilidade de detecção, enquanto as que formam  $45^\circ$  têm 50%; col. 6: Chave formada pelos bits das posições em que o fóton foi detectado.

Novamente, é isto o que garante a segurança do protocolo. Como a codificação escolhida por A (Alice) não é ortogonal, é impossível medir simultaneamente se o fóton está polarizado verticalmente ou em diagonal  $+45^\circ$ . Na física clássica, se incidimos uma luz polarizada em diagonal  $+45^\circ$  em um polarizador vertical, há um corte de 50% da intensidade da luz; no entanto, na física quântica, o resultado é booleano (quantizado) e probabilístico: há 50% de probabilidade de o fóton ser detectado, e a medida perturba o estado do fóton.

## 12.13 Protocolo BBM92

No protocolo de (**Bennett-Brassard**) ([BENNETT; BRASSARD, 1984](#)) pode-se simplificar ainda mais o protocolo anterior ([BENNETT; WIESNER, 1992](#)). Agora, ao invés de Alice e Bob orientarem seus detectores aleatoriamente em três direções, eles necessitam apenas de duas direções. Eles orientam seus polarizadores ou na direção x ou na direção y. Note que ambas as direções formam um ângulo de  $90^\circ$ . Novamente, Alice e Bob anunciam publicamente a orientação de cada polarizador em cada medida. No entanto, eles não informam os resultados. Em seguida, eles descartam todas as medidas nas quais foram utilizadas orientações diferentes. São mantidos apenas os eventos cujos polarizadores foram orientados numa mesma direção. Se Eva não interferiu, toda medida onde ambos utilizaram uma mesma direção para seus polarizadores deve estar anti-correlacionada. O leitor pode ver a explicação detalhada deste protocolo em ([RIGOLIN; RIEZNIK, 2005](#)).

## 12.14 Oblivious Transfer Protocol - Transferência Inconsciente

A ideia de transferência inconsciente (em inglês, *Oblivious Transfer, OT*) nos parece um assunto para a conjuntura jurídica atual é uma troca de mensagens entre 2 pessoas que não confiam uma na outra: A (Alice), que envia as mensagens, e B (Bob), que recebe. Nesta troca, A envia duas mensagens iguais, e tem uma chance

de 50% de conseguir enviar cada uma. Caso uma delas consiga ser enviada com sucesso, somente B (Bob) saberá se ela foi enviada com sucesso ou não (BENNETT et al., 1992). Isto foi desenvolvido para que essas duas pessoas possam resolver algum problema que eles tenham em comum, sem revelar informações desnecessárias para a resolução do mesmo e sem a necessidade de um terceiro mediador.

Há vários protocolos de transferência inconsciente na computação clássica, que utilizam criptografia assimétrica; no entanto, estes só conseguem garantir a segurança contra ataques externos ou trapaças a um dos participantes desta comunicação (WOLF; WULLSCHLEGER, 2005). Já os protocolos quânticos de OT são capazes de garantir um alto grau de confiabilidade para os dois participantes da comunicação; mostramos um destes protocolos a seguir.

Neste protocolo, A (Alice) codifica um bit no produto do *spin* de duas partículas. A (Alice) envia essas duas partículas para B (Bob), e B (Bob) escolhe medir sua polarização no eixo x ou no eixo y. Então ele diz a A (Alice) se as medidas foram feitas com sucesso. Caso a resposta seja não, A (Alice) reenvia as duas partículas e B (Bob) repete o processo de medição; caso contrário, A (Alice) conta qual base foi escolhida para o *spin* das partículas usadas para codificar o bit (ARDEHALI, 1995).

Este protocolo tem um alto grau de segurança, pois caso B tente de alguma forma trapacear medindo uma partícula em um eixo e a segunda em outro eixo, a probabilidade de ele ser bem sucedido é ínfima. Também não é possível, para B, trapacear armazenando os fons antes do último passo, pois não é possível fazer isso. Pode-se considerar, também, a utilização de EPR, que é efetivo, mas não é implementável com a tecnologia atual.

## 12.15 Criptografia quântica para acesso em Big Data

### A Quantum Cryptography Protocol for Access Control in Big Data

**2018** - Uma perspectiva conceitual do influxo de dados de diversas fontes de dados que atravessam redes através de canais de comunicação é apresentado em (ODEDOYIN, 2018). Um *framework* prevê diferentes fontes de dados que geram um aumento no volume de dados. Esses dados são heterogêneos (variedade), compreendendo dados não estruturados, semi-estruturados e estruturados sendo transferidos a velocidades variadas (velocidade) de um lado para o outro. A Figura 210 exibe a visão geral conceitual do Big Data na transmissão.

Neste trabalho, um protocolo de criptografia quântica (ODEDOYIN, 2018) é proposto para controle de acesso a Big Data. Este protocolo está ativo nas etapas de troca de chaves e filtragem de chaves. O fluxo de Big Data foi conceituada e uma formalização geral foi feita para o protocolo. Um *framework* foi suportado fora das etapas envolvidas na criptografia quântica para a realização do protocolo. Esta pesquisa é um trabalho em andamento que promete um protocolo para controle de acesso em Big Data. Mais distante, a pesquisa abordará a verificação de protocolos, simulação e avaliação do protocolo.

## 12.16 Six-State Protocol

O **Protocolo Six-State** - Diferente do que foi proposto no BB84 e no B92, onde foi mostrado que dois estados bastam, mas quatro é o padrão, pode ser usado

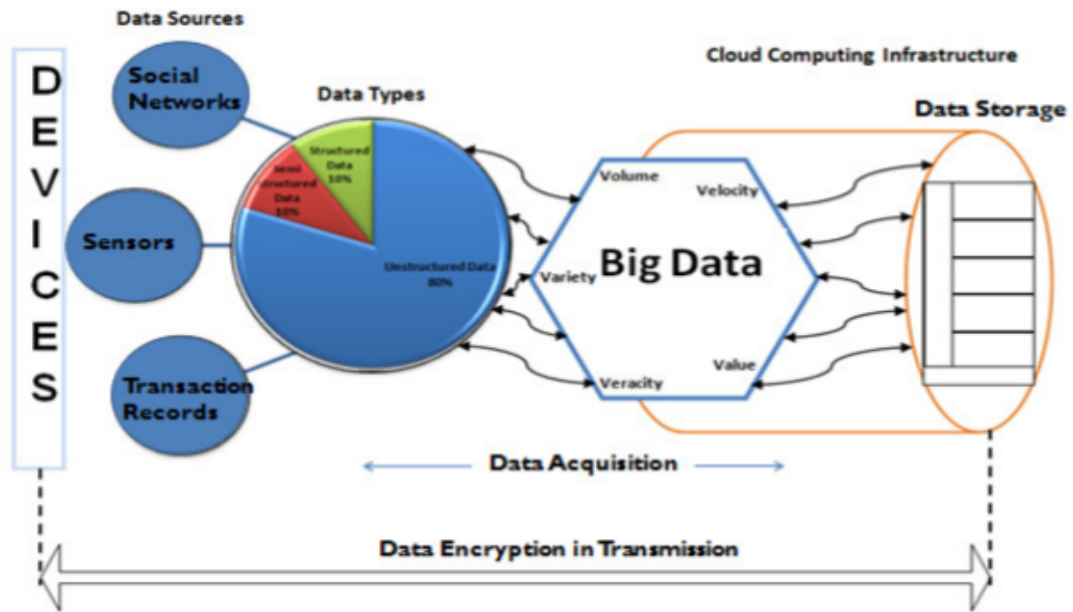


Figure 1: Conceptual overview of the flow of big data

Figura 210 – Criptografia Quântica para controle de acesso à Big Data.

Fonte: (ODEDOYIN, 2018)

um protocolo de 6 estados (SULZBACH, 2003).

## 12.17 Tecnologias para a Criptografia Quântica

Atualmente, a criptografia quântica não é mais somente teoria. Ela já foi implementada em diversos laboratórios e em algumas redes de teste feitas por empresas. As implementações existentes seguem o modelo de ter LEDs ou lasers como fontes de luz, utilização de filtros e polarizadores de luz para garantir o fluxo de alguns poucos fótons, e detectores no receptor. Já em relação ao canal quântico, há dois modos diferentes em funcionamento: a transmissão de fótons pelo ar (BENNETT et al., 1992) e por fibra ótica (STIX, 2005).

A aplicação da teoria da Criptografia Quântica já foi realizada em laboratório entre outros pela IBM. Porém apenas se obtiveram resultados satisfatórios para distâncias curtas entre o emissor e o receptor. Conseguiu-se que com cabos de fibra ótica de elevada pureza se comunicasse a uma distância que ronda os 70km. A uma distância maior, a taxa de erros de bits, causados pelo **Princípio da Incerteza de Heisenberg** e por impurezas microscópicas na fibra ótica, cresce e inviabiliza a aplicabilidade do método. Também foi testada a comunicação pelo ar, sendo que esta apenas foi bem sucedida com distâncias na ordem das centenas de metros e com condições climáticas ideais. Espera-se que o desenvolvimento tecnológico permita fazer crescer estas distâncias.

No entanto, apesar de já ser possível utilizar a criptografia quântica, a tecnologia disponível não consegue fornecer canais quânticos com comprimentos o suficiente para fazer qualquer tipo de conexão (o máximo que se atinge são algumas centenas de

quilômetros). A solução encontrada seria conseguir fazer algum tipo de "retransmissor quântico", que retransmitiria o sinal em intervalos de distâncias pré-definidos. No entanto não se conseguiu fazer isso ainda (STIX, 2005).

Para fazer esse "retransmissor quântico" os cientistas estão se baseando num fenômeno chamado *emaranhamento* (GISIN, 2002). A ideia consiste em emaranhar dois fótons de dois cabos de fibra ótica diferentes para que eles possam transmitir a informação de um terceiro fóton entre os dois cabos. Já houve alguns experimentos bem sucedidos (STIX, 2005), então podemos esperar que futuramente essa ideia possa ser implementada comercialmente.

Algumas empresas já vendem formas de implementação de criptografia quântica. A idQuantique <<http://swissquantum.idquantique.com/>> (2011) e a MagiQ Technologies <[http://www.magiqtech.com/MagiQ/Products\\_files/8505\\_Data\\_Sheet.pdf](http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf)> (2007) já oferecem o serviço com transmissão de fótons pela fibra ótica. A "iD Quantique" (Suíça) comercializa a (OMER, 2009) aparelhos que efetuam criptografia quântica. A QinetiQ <<http://www.qinetiq.com/pages/default.aspx>> (2011) oferece com a transmissão de fótons pelo ar. A "NOW Wireless" <<https://nowwireless.com/>> celebrou um contrato para distribuir o "gateway MagiQ QPN", uma solução de criptografia quântica que permite a comunicação a mais de 120km de distância.

Segundo a revista "New Scientist", nos EUA (Cambridge, Massachusetts) um projeto chamado "Quantum Network (Qnet)", financiado pela "Defense Advanced Research Projects Agency" foi executado. Atualmente este projeto dispõe de seis servidores, mas que se podem ligar a outros servidores através da Internet e usando Criptografia Quântica. O objectivo deste projeto é utilizar esta tecnologia em empresas de crédito, bancos e outros serviços financeiros que possibilitem aos seus clientes transações eletrônicas. A rede tem 10Km de extensão e liga a empresa BBN à Universidade de Harvard através de cabos de fibra ótica comuns.

## 12.18 Quantum money - O futuro

*Quantum money* (dinheiro quântico) é um projeto proposto de notas de banco, tornando-as impossíveis de forjar, usando a física quântica.

Além de um número de série único em cada nota de banco (essas notas são na verdade mais parecidas com cheques, já que uma etapa de verificação com o banco é necessária para cada transação), há uma série de sistemas quânticos isolados de dois estados (LO; POPESCU, 1998). Por exemplo, fótons em uma das quatro polarizações poderiam ser usados: a  $0^\circ$ ,  $45^\circ$ ,  $90^\circ$  e  $135^\circ$  para algum eixo, que é referido como a vertical. Cada um deles é um sistema de dois estados em uma das duas bases: a base horizontal tem estados com polarizações a  $0^\circ$  e  $90^\circ$  com a vertical, e a base diagonal tem estados a  $45^\circ$  e  $135^\circ$  com a vertical.

No banco, há um registro de todas as polarizações e os números de série correspondentes. Na nota de banco, o número de série é impresso, mas as polarizações são mantidas em segredo. Assim, enquanto o banco pode sempre verificar as polarizações medindo a polarização de cada fóton na base correta sem introduzir qualquer perturbação, um possível falsificador ignorante das bases não pode criar uma cópia dos estados de polarização de fótons, pois mesmo que ele saiba as duas bases, se ele escolher o errado para medir um fóton, mudará a polarização do fóton na armadilha,

e a nota falsificada criada será com essa polarização errada.

Para cada fóton, o possível falsificador tem uma probabilidade de duplicar o sucesso corretamente. Se o número total de fótons na nota de banco for  $N$ , uma duplicata terá probabilidade  $(3/4)^N$  de passar a verificação do banco teste. Se  $N$  for grande, essa probabilidade se tornará exponencialmente pequena. O fato de que um estado quântico não pode ser copiado é, em última instância, garantido por sua prova pelo *teorema da não-clonagem*, subjacente à segurança desse sistema.

## 12.19 Desafios na Comunicação com Criptografia Quântica

Sendo esta uma área recente e em expansão possui muitos desafios teóricos e práticos que necessitam de ser enfrentados para que as comunicações quânticas possam crescer. Alguns dos principais desafios são:

- Desenvolvimento de fontes de um fóton de tamanho reduzido e baixo custo.
- Desenvolvimento de repetidores quânticos para aumentar o alcance entre os utilizadores de uma rede quântica.
- Desenvolvimento de novos protocolos de criptografia quântica usando sistemas quânticos de mais de dois estados.
- Desenvolver protocolos de distribuição de chave pública, autenticação e assinatura digital.
- Promover a integração da rede quântica com a infra-estrutura atualmente existente.
- Formar hackers quânticos para testar a segurança dos protocolos.

## 12.20 Tipos de criptografia quântica

Os tipos de criptografia quântica que podem ser construídas, na Figura 211:

## 12.21 Recomendações

Neste capítulo foi apresentado de maneira acessível ao leitor leigo em criptografia quântica, os quatro protocolos de distribuição de chaves quânticas que fundaram a área da criptografia quântica em 1984.

O primeiro deles, o protocolo BB84, é recomendado também como texto introdutório a esse assunto. Devido ser o trabalho pioneiro, considera-se (BENNETT; BRASSARD, 1984) uma ótima opção para se introduzir criptografia quântica a estudantes de graduação em Física, Ciência da Computação ou outros cursos afins.

O protocolo E91 requer um pouco mais de conhecimento do leitor. Contudo, com um pouco de esforço e uma introdução às desigualdades de Clauser, Horne, Shimony e Holt (CLAUSER et al., 1969), ele também pode ser aprendido durante um curso de graduação em Física ou Ciência da Computação.



Figura 211 – Tipos de criptografia viáveis de ser construídas.

Fonte: <<https://www.cryptoradar.com.br/tecnologia/a-computacao-quantica-pode-protect-discretionary{\char\hyphenchar\font}{\font}}{-destruir-as-criptomoedas/>>>

Os outros dois protocolos, BBM92 e B92, por se tratarem de extensões e simplificações dos protocolos anteriores, são facilmente entendidos por leitores que já dominaram o assunto dos primeiros dois protocolos.

Enfim, acreditamos na viabilidade de se ensinar criptografia quântica durante cursos de graduação. E mais, ensinar criptografia quântica pode ser também extremamente vantajoso para convencer um maior número de pessoas, da importância da mecânica quântica.

## 12.22 Bibliografia e Fonte de Consulta

In Wikimedia Foundation, *Criptografia quântica*. Disponível em: <[https://pt.wikipedia.org/wiki/Criptografia\\_quântica](https://pt.wikipedia.org/wiki/Criptografia_quântica)>, Acesso em: 15 de maio de 2019.

Gustavo Rigolin e Andrés Anibal Rieznik - *Introdução à criptografia quântica*. Revista Brasileira de Ensino de Física, v. 27, n. 4, p. 517-526, 2005.

In Wikimedia Foudation. *Quantum Money*. Disponível em: <[https://en.wikipedia.org/wiki/Quantum\\_money](https://en.wikipedia.org/wiki/Quantum_money)>. Acesso em Maio 28,2019.

In Wikimedia Foundation, Stephen Wiesner. Disponível em: <[https://en.wikipedia.org/wiki/Stephen\\_Wiesner](https://en.wikipedia.org/wiki/Stephen_Wiesner)>, Acesso em Maio 28,2019.

Abiodun O. Odedoyin, Helen O. Odukoya, Ayodeji O. Oluwatope - *A Quantum Cryptography Protocol for Access Control im Big Data*. International Journal on Cryptography and Information Security (IJCIS), Vol. 8, No.2, June 2018.

In Wikimedia Foudation. *Oblivious Transfer*. Disponível em: <[https://en.wikipedia.org/wiki/Oblivious\\_transfer](https://en.wikipedia.org/wiki/Oblivious_transfer)>, Acesso em 28 de maio de 2019.

Simon Singh. *O Livro dos Códigos*. [S.l.]: Record, pp. 367-68, 2000, ISBN 8501055980.

Charles Bennett - Disponível em: <<http://www.research.ibm.com/people/b/bennet/>>. Acesso em: 28 de maio de 2019.

Artigo publicado por Charles Bennett e Gilles Brassard com o título Criptografia quântica: a distribuição de chaves públicas e lançamento de moedas (em inglês), <<http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf>>, 1984.

Teletransporte-Quântico - Fapesp <<http://www.agencia.fapesp.br/materia/10006/divulgacao-cientifica/teletransporte-quantico.htm>>

Physicists double their teleportation power - Quantum technique transfers two photon properties por ANDREW GRANT em 25 de fevereiro de 2015.

"Profile: John Smolin, American Physical Society.

Bennett, Charles H.; DiVincenzo, David P.; Smolin, John A.; Wootters, William K. (1996), "Mixed State Entanglement and Quantum Error Correction", *Phys. Rev. A* 54: 3824-3851

D.P. DiVincenzo, P.W. Shor, and J. A. Smolin, "Quantum-channel capacity for very noisy channels", *Phys. Rev. A*, 1717 (1999)

Bennett, Bessette, Brassard Salvial, and Smolin "Experimental Quantum Cryptography", *Journal of Cryptology* 5, 3-28 (1992)

"Church of the Larger Hilbert Space" article in Quantiki

John Smolin's blog - <<http://john.kangry.com/>>

Fundamentos de algoritmia. Gilles Brassard & Paul Bratley. ISBN 848966000X.

Bennett, Brassard: Quantum Cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore, 1984, P. 175.

C. H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres und W. K. Wootters: Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. In: Physical Review Letters. Band 70, 1993, p. 1895.

Gilles Brassard (em inglês) no Mathematics Genealogy Project (<[https://pt.wikipedia.org/wiki/Mathematics\\_Genealogy\\_Project](https://pt.wikipedia.org/wiki/Mathematics_Genealogy_Project)>).

Página oficial de Gilles Brassard - <<http://www.iro.umontreal.ca/~brassard/>>, Acesso em Maio 08, 2017.

**Quantum Cryptography Roadmap** - <[http://qist.lanl.gov/qcrypt\\_map.shtml](http://qist.lanl.gov/qcrypt_map.shtml)>.

## 12.23 Referências e Leitura Recomendada

The first paper ever published on this: Bennett, C. H., Brassard, G., Breidbart, S. and Wiesner, S., "Quantum cryptography, or unforgeable subway tokens", Advances in Cryptology: Proceedings of Crypto 82, August 1982, Plenum Press, pp. 267-275. A listing of a huge number of quantum cryptography papers, with some discussion of them, is at <<http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html>>

A primeira publicação no assunto: Wiesner, S. "Conjugate Coding" SIGACT News, Vol. 15, 1983, pp. 7888; Brassard, G. and Bennett, C.H., Proceedings of the IEEE International Conference on Computer Systems and Signal Processing, 1984, p. 175 Ekert, A. "Quantum Cryptography Based on Bell's Theorem" Physical Review Letters, Vol. 67 1991 pp. 661663.

BENNETT, C. H, Brassard, G. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984 (IEEE, New York, 1984), pp. 175-179; IBM Tech. Discl. Bull. 28, 3153-3163, 1985.

Provably Secure - <[https://en.wikipedia.org/wiki/Provable\\_security](https://en.wikipedia.org/wiki/Provable_security)>

Quantum Key Distribution - <[https://en.wikipedia.org/wiki/Quantum\\_key\\_distribution](https://en.wikipedia.org/wiki/Quantum_key_distribution)>

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

C.E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, vol.28-4, (1949) pp.656-715.

Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves (PDF). Centro Brasileiro de Pesquisas Físicas, Serie Monografias, 2003. Consultado em 6 de fevereiro de 2009.

Protocols and Privacy Amplification - <[www.quadibloc.com/crypto/mi060703.htm](http://www.quadibloc.com/crypto/mi060703.htm)>

Quantum Cryptographic Protocols - <<https://www.perimeterinstitute.ca/personal/dgottesman/crypto.html>>



Quantum Key Distribution -

<<https://cdn.ymaws.com/www.issa.org/resource/resmgr/journalpdfs/feature0612.pdf>>

Quantum Key Distribution -

<<https://www.quantiki.org/wiki/quantum-key-distribution>>

Bibliografia de Criptografia Quântica - <<http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html>>

Quantum Cryptography in Norway - <http://www.vad1.com/lab/>

# Posfácio

A Série Pensamento Matemático @ Ciência da Computação - O presente volume (o terceiro desta série) abordou os personagens e as suas grandes ideias que fizeram surgir a Ciência da Computação Quântica. Iniciando com fatos históricos nos tempos da Física clássica, a partir das limitações da mesma, mostrou o surgimento da Física quântica, passando pela aplicação da matemática de **David Hilbert** e **John von Neumann** para modelar sistemas quânticos, e finalizou destacando os os circuitos quânticos da computação quântica e os protocolos mais conhecidos de criptografia quântica.

Mediante esses três exemplos de algoritmos quânticos (**Deutsch**, **Shor** e **Grove**), percebe-se que computadores quânticos poderão, de fato, revolucionar a forma como tratamos a informação, sendo necessário, para isso, que novos algoritmos quânticos sejam elaborados. Este é um grande desafio para o futuro da ciência da computação (**NIELSEN; CHUANG, 2010**).

Todas as partes deste volume III, **Computação Quântica: Aspectos Físicos e Matemáticos - Uma Abordagem Algébrica**, contém capítulos organizados numa ordem natural, em que os autores imaginam poder facilitar o leitor a entender e se situar num contexto que redunde na computação quântica, desde as raízes da Física quântica, passando pelos circuitos quânticos, e chegando aos algoritmos quânticos (um processamento de circuitos quânticos) e sua complexidade computacional.

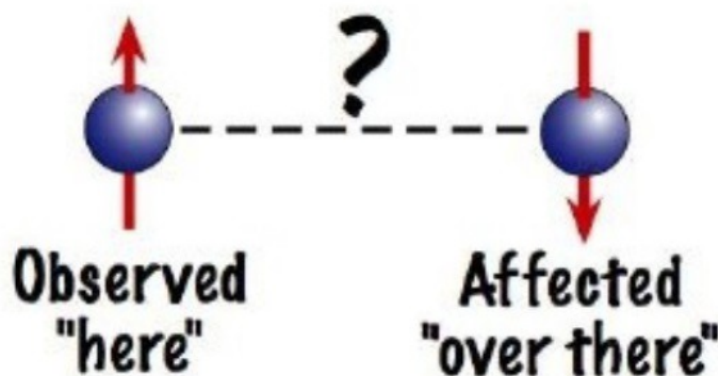


Figura 212 – Como no emaranhamento quântico ...

Fonte: BQP-Wikipedia, a enciclopédia livre em <<https://pt.wikipedia.org/wiki/BQP>>

Para dar seguimento à série **Pensamento Matemático @ Ciência da Computação**, além deste volume, o leitor é então, convidado a acompanhar os futuros

volumes da *Série Pensamento Matemático @ Ciência da Computação*, afim de conhecer as pesquisas que redundaram no avanço desta fantástica ciência quântica. Os personagens, as grandes ideias e os fatos marcantes na computação quântica, proporcionarão outros volumes.

Durante o levantamento bibliográfico para este trabalho, além desta vertente (1) da abordagem algébrica para a computação quântica (Hilbert/John von Neumann), foram encontradas outras vertentes que não puderam ser seguidos e estudados durante a construção deste livro. A **lógica paraconsistente**, as **máquinas de Turing paraconsistentes**, as **máquinas de Turing quânticas** e os **circuitos quânticos** são os assuntos para uma **abordagem lógica** para a computação quântica.

Trata-se (2) da abordagem da **lógica paraconsistente** para a computação quântica, que se ocupa das máquinas de **Turing** paraconsistentes e das máquinas de Turing quânticas, até chegarmos aos circuitos quânticos, em contraste com a abordagem algébrica; (3) referente a vertente do estudo dos algoritmos quânticos e suas complexidades computacionais; (4) o estudo das linguagens de programação quânticas. Estes quatro assuntos foram ventilados, durante a elaboração deste volume, mas diante da complexidade do tema, somente (1) é aqui apresentado, podendo (2), (3) e (4), virem a ser outros três volumes desta série.

Depois de todo esse material, é conveniente que se faça um resumo de todos esses conceitos, destacando o que é fundamental. Mas, deixamos para os interessados no tema, que ao ler este conteúdo, possa destacar esses conceitos a seu gosto.

Para aqueles que quiserem um livro sobre Mecânica Quântica Básica, recomendo estudar em ([NOVAES; STUDART, 2016](#)).

Florianópolis, Julho de 2019

João Bosco M. Sobral  
Departamento de Informática e Estatística da UFSC

# Referências

- AGRAWAL, M.; KAYAL, N.; SAXENA, N. Primes is in p. *Annals of Mathematics*, v. 160, n. 2, p. 781–793, 2004. Disponível em: <<http://annals.math.princeton.edu/2004/160-2/p12>>. Citado 2 vezes nas páginas 180 e 257.
- ALBERT, D. Z. On quantum-mechanical automata. *Physics Letters A*, v. 98, p. 249–252, 1983. On behalf of the Philosophy of Science Association. Citado na página 212.
- ALMEIDA, V. L. d. *Os Teoremas de Sturm e Geometria Simplicita*. 24 p. Dissertação (Mestrado), 2012. Disponível em: <<http://www.mat.ufmg.br/intranet-atual/pgmat/TesesDissertacoes/uploaded/Diss198.pdf>>. Citado na página 180.
- ALVES, F. L. *Computacao Quantica: Fundamentos Fisicos e Perspectivas*. [S.l.], 2003. Citado na página 250.
- ALVES, L. *Michael Faraday*. 2017. Disponível em: <<https://brasilecola.uol.com.br/quimica/michael-faraday.htm>>. Citado na página 9.
- AMARAL, E. *Operadores Lineares em Espacos de Hilbert e Aplicacoes*. Dissertação (Dissertacao (mestrado)), 2006. Citado 2 vezes nas páginas 121 e 130.
- AMSLER, C. *The origin of the word "photon"*. 2008. Citado na página 56.
- ARDEHALI, M. *A simple quantum oblivious transfer protocol*. 1995. Citado na página 291.
- ARORA, S.; BARAK, B. *Computational Complexity: A Modern Approach*. 2007. Cambridge University Press. Citado na página 264.
- ATKINSON, P. A. *O Algoritmo Quantico de Shor*. [s.n.], 2001. Disponível em: <[https://www.ime.usp.br/~yw/ano2001/5701/sem2/patk\\_relfinal.pdf.gz](https://www.ime.usp.br/~yw/ano2001/5701/sem2/patk_relfinal.pdf.gz)>. Citado 2 vezes nas páginas 258 e 259.
- AZAMBUJA, E. *A sobreposicao quantica macroscopica saira do papel?* 2016. Disponível em: <<http://www.electronicsspecifier.com.br/noticias-da-industria/a-sobreposicao-quantica-macroscopica-saira-do-papel>>. Citado na página 217.
- BAGGOT, J. *Beyond Measure - Modern Physics, Pylosophy and the Meaning of Quantum Theory*. [S.l.]: Oxford University Press, 2004. Citado na página 94.

BALLENTINE, L. *Quantum Mechanics: A Modern Development*. [S.l.: s.n.], 1998. ISBN 9810241054. Citado na página 38.

BELL, J. S. *The Speakable and Unspeakable in Quantum Mechanics*. [S.l.]: Cambridge University Press, 1987. Citado na página 92.

BENNETT et al. Experimental quantum cryptography. *J. of Cryptology*, v. 5, p. 3–28, 1992. Citado 3 vezes nas páginas 286, 291 e 292.

BENNETT, C. Logical reversibility of computation. *IBM J. Res. Dev.*, 1973. Citado na página 210.

BENNETT, C.; WIESNER, S. J. *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*: Phys. rev. lett. 1992. 69:2881. Citado 4 vezes nas páginas 272, 288, 289 e 290.

BENNETT, C. H. Mixed state entanglement and quantum error correction. *Phys. Rev. A.*, v. 54, p. 3824–3851, 1996. DiVincenzo, D. P. and Smolin, J. A. and Wootters, W. K. Citado 2 vezes nas páginas 278 e 285.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing 9 (Bangalore, India, 1984)*, v. 1 of 3, p. 175–179, 1984. Disponível em: <<https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>>. Citado 6 vezes nas páginas 272, 278, 282, 289, 290 e 294.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computers, Systems and Signal Processing*, 1984. Citado 3 vezes nas páginas 234, 282 e 289.

BERNSTEIN, D. J. Detecting perfect powers in essentially linear time. *Math. Comp.*, v. 67, n. 223, p. 1253–1283, 1998. Citado na página 257.

BOLDRINI, J. L. et al. *Algebra Linear*. [S.l.]: HARBRA Ltda, 1980. Citado na página 166.

BOURBAKI, N. *Elements of Mathematics, Algebra I*. [S.l.]: Spring-Verlag, 1989. ISBN 3-540-64243-9. Citado na página 172.

BRUMATTO, H. J. *Introducao a Computacao Quantica*. 2012. RA 096389. Disponível em: <<http://www.ic.unicamp.br/~ducatte/mo401/1s2010/T2/096389-t2.pdf>>. Citado 11 vezes nas páginas 214, 222, 223, 224, 227, 228, 229, 230, 231, 232 e 236.

BUTKOV, E. *Mathematical Physics*. [S.l.]: Addison Wesley Publishing Company Inc., 1968. Citado na página 166.

CABRAL, G.; LIMA, A.; LULA, B. Interpretando o algoritmo de deutsch no interferometro de mach-zehnder. *Revista Brasileira de Ensino de Fisica*, v. 26, n. 2, p. 109–116, 2004. Citado na página 262.

- CABRAL, G. E. M.; JR, B. L.; LIMA, A. F. Zeno a new graphical tool for design and simulation of quantum circuits. In: DONKOR, E. J.; PIRICH, A. R.; BRANDT, H. E. (Ed.). *In Proceedings of SPIE, Conference Quantum Information and Computation III*. [S.l.: s.n.], 2005. v. 5815, p. 127–137. Citado na página 245.
- CALLIOLI, C. A.; DOMINGUES, H. H.; COSTA, R. C. F. *Algebra Linear e Aplicacoes*. 6 ed.. ed. [S.l.: s.n.], 1990. P. 77. ISBN 9788570562975. Citado na página 143.
- CARDONHA, C. H.; SILVA, M. K. C.; FERNANDES, C. G. *Computacao Quantica: Complexidade e Algoritmos*. [S.l.], 2004. Ago/2003- Dez/2004. Citado 14 vezes nas páginas 111, 112, 144, 148, 149, 152, 171, 173, 174, 180, 189, 257, 259 e 264.
- CARNIELLI, W. *Paraconsistencia e Computacao Quantica*. 2010. Disponível em: <[http://qubit.lncc.br/weciq/pdf/WECIQ2010\\_Walter\\_Carnielli.pdf](http://qubit.lncc.br/weciq/pdf/WECIQ2010_Walter_Carnielli.pdf)>. Citado na página 131.
- CASSIDY, D. C. *Exhibit on Werner Heisenberg*. American Institute of Physics, 1998. Disponível em: <[http://www.aip.org/history/heisenberg/p09\\_text.htm](http://www.aip.org/history/heisenberg/p09_text.htm)>. Citado na página 41.
- CHAICHIAN, M.; DEMICHEV, A. P. *Introduction to Path Integrals in Physics*. [S.l.: s.n.], 2001. Citado na página 70.
- CHUANG, I. L. Nmr quantum computing: Realizing shor s algorithm. *Nature Journal*, p. 883–887, 2001. Citado na página 181.
- CHURCH, A. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, v. 58, n. 2, p. 345–363, 1936. Disponível em: <<https://www.ics.uci.edu/~lopes/teaching/inf212W12/readings/church.pdf>>. Citado na página 206.
- CIRAC, J. I.; ZOLLER, P. Quantum computations with cold trapped ions. *Physical Rev. Lett.*, n. 74, p. 4091, 1995. Citado na página 181.
- CLAUSER, J. F. et al. *Physical Review. Letter*. 1969. 23, 880. Citado 2 vezes nas páginas 278 e 294.
- CLEVE, R. et al. Quantum algorithms revisited. *A Math. Phys. Eng. Sci.*, v. 454, n. 1969, p. 339–354, 1998. Citado na página 262.
- COBO, M. F.; ZANATTA, A. R. *Constante de Planck*. 2013. Disponível em: <[http://www.ifsc.usp.br/~lavfis/images/BDApostilas/ApConstantePlanck/CtePlanck\\_1.pdf](http://www.ifsc.usp.br/~lavfis/images/BDApostilas/ApConstantePlanck/CtePlanck_1.pdf)>. Citado na página 10.
- COHEN-TANNOUJDI, C.; DIU, B.; LALOE, F. *Quantum Mechanics*. [S.l.]: John Wiley Interscience, 1992. v. 1. Citado na página 184.
- CORMEN, T. H. et al. *Introduction to Algorithms*. Second editon. [S.l.]: MIT Press, Cambridge, 2001. MA. Citado na página 214.

COURTEILLE, W. Mecânica quântica. Acesso em: 28 Fev. 2018. 2017. Citado na página 160.

DALMOLIN, C. *Química Quântica - Postulados da Mecânica Quântica*. 2010. Disponível em: <[http://www.joinville.udesc.br/portal/professores/carlad/materiais/05\\_Postulados.pdf](http://www.joinville.udesc.br/portal/professores/carlad/materiais/05_Postulados.pdf)>. Citado na página 170.

DEUTSCH, D. Quantum theory, the church-turing principle and the universal quantum computer. *A*, n. 400, p. 97–117, 1985. Citado 9 vezes nas páginas 180, 204, 205, 207, 208, 209, 210, 212 e 262.

DEUTSCH, D. Quantum theory, quantum computational networks. *Proceedings of Royal Society of London*, v. 425, p. 73–90, 1989. Citado na página 212.

DEUTSCH, D.; JOZSA, R. Rapid solution of problems by quantum computer. v. 439, p. 553–558, 1992. Citado na página 180.

DIEKS, D. *Physical Letter*. 1982. A 92, 271. Citado na página 285.

DIRAC, P. A. M. *The Lagrangian in Quantum Mechanics*. [S.l.]: Physikalische Zeitschrift der Sowjetunion, 1933. Citado na página 71.

DIRAC, P. A. M. A new notation for quantum mechanics. In: *In Mathematical Proceedings of the Cambridge Philosophical Society*. [S.l.]: Cambridge University Press, 1939. v. 35, p. 416–418. Citado 4 vezes nas páginas 148, 156, 161 e 217.

DIVINCENZO, D. P.; SHOR, P. W.; SMOLIN, J. A. Quantum-channel capacity for very noisy channels. *Physical Review A*, v. 1717 (1999), 1999. Citado na página 286.

EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physical reality be considered complete? *Institute for Advanced Study*, n. 47, p. 777–780, 1935. Princeton, New Jersey, USA. Citado na página 41.

EISBERG, R.; RESNICK, R. *Física Quântica*. [S.l.: s.n.], 1979. Citado na página 41.

EISBERG, R.; RESNICK, R. *Física Quântica: Átomos, Moléculas, Sólidos, Núcleos e Partículas*. [S.l.]: Elsevier, 1979. 19-42 p. Citado na página 184.

EKERT, A.; HAYDEN, P. M.; INAMORI, H. Basic concepts in quantum computation, vol. 72/2001 of *Les Houches. Springer Berlin*, 2001. Citado 3 vezes nas páginas 215, 217 e 226.

EKERT, A. K. *Physical Review Letter*. 1991. 67, 661. Citado na página 278.

EXEL, R. *Von Neumann e a Teoria de Algebras de Operadores*. 1996. Disponível em: <<http://mtm.ufsc.br/~exel/papers/vn.pdf>>. Citado na página 128.

FALCAO, G. B. N.; MOLINARI, R. Historico, estado e perspectivas da tecnologia da computacao quantica. *RUEP- Revista UNILUS Ensino e Pesquisa*, v. 13 ISSN 2318-2083 (eletrônico), n. 31, p. 88–100, 2016. ISSN 2318-2083. Disponível em: <<https://revista.unilus.edu.br/index.php/ruep/article/download/745/u2016v13n31e745>>. Citado na página 250.

FERNANDES, F. *Topicos de Mecanica Quantica I - Equacoes de Newton e de Hamilton versus Equacoes de Schrodinger*. 2010. Notas para as aulas de Química-Física II, 2010/11. Disponível em: <[http://webpages.fc.ul.pt/~fmfernandes/Papers/T6\\_MecQuantica\\_1.pdf](http://webpages.fc.ul.pt/~fmfernandes/Papers/T6_MecQuantica_1.pdf)>. Citado 2 vezes nas páginas 161 e 162.

FEYNMAN, R. P. *The Feynman Lectures on Physics: Quantum Mechanics*. [S.l.]: Addison-Wesley, 1982. v. 1-14. Citado na página 184.

FEYNMAN, R. P. Simulating physics with computers. *Journal of Theoretical Physics*, 1982. Citado na página 210.

FEYNMAN, R. P. Quantum mechanical computers. *Optics News*, n. 11, p. 11–20, 1985. Citado na página 180.

FEYNMAN, R. P. *Licoes de Fisica de Feynman*. [S.l.: s.n.], 2008. 1-12 p. Citado na página 41.

FEYNMAN, R. P. *Quantum Mechanics and Path Integrals*. [S.l.: s.n.], 2010. Citado na página 70.

FREIRE, O. J.; PESSOA, O. J.; BROMBERG, J. L. *Teoria Quantica: estudos historicos e implicacoes culturais*. [S.l.]: Editora da Fisica, 2010. Citado na página 184.

FREITAS, A. X. *Algoritmo de Shor e sua aplicacao a fatoracao de numeros inteiros*. Dissertação (Dissertacao de mestrado), 2010. Disponível em: <<https://www.ime.unicamp.br/~tcunha/Diss/DisAdriana.pdf>>. Citado na página 256.

GALLAS, J. Atomos de rydberg. *Cad. Cat. Ensino de Fisica*, v. 3, n. 1, p. 41–45, 1986. UFSC. Disponível em: <<https://periodicos.ufsc.br/index.php/fisica/article/viewFile/7937/7303>>. Citado na página 17.

GANDY, R. O. *On axiomatic systems in mathematics and theories in physics*. Tese (phdthesis), 1953. Citado na página 207.

GANDY, R. oliver. Church's thesis and principles for mechanisms. *In The Kleene Symposium*, . pp., p. 123–148, 1980. Citado na página 207.

GERSHENFELD, N.; CHUANG, I. L. Quantum computing with molecules. *Scientific American*, p. 66–71, 1998. Disponível em: <<http://cba.mit.edu/docs/papers/98.06.sciqc.pdf>>. Citado 2 vezes nas páginas 244 e 247.



- GISIN, N. Quantum cryptography. *Reviews of Modern Physics*, n. 74, 2002. Citado na página 293.
- GOUVEIA, T. da C. *Polinomios de Hermite - Uma Aplicacao na Mecanica Quantica*. Dissertação (Trabalho de conclusao de curso), 2014. Citado na página 131.
- GRIFFITHS, D. J. *Introduction to Quantum Mechanics*. (2nd ed.). [S.l.: s.n.], 2004. ISBN 0-13-111892-7. Citado 2 vezes nas páginas 38 e 46.
- GROVER, L. K. A fast quantum mechanical algorithm for database search. p. 212, 1996. Disponível em: <<https://arxiv.org/abs/quant-ph/9605043>>. Citado 2 vezes nas páginas 247 e 259.
- GROVER, L. K. Quantum computing: How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today. *The Sciences*, 1999. Disponível em: <<https://cryptome.org/qc-grover.htm>>. Citado na página 247.
- GROVER, L. K. From schrodinger's equation to quantum search algorithm. *American Journal of Physics*, v. 69, n. 7, p. 769–777, 2001. Disponível em: <<https://arxiv.org/abs/quant-ph/0109116>>. Citado na página 247.
- HEISENBERG, W. (Ed.). *Uber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*. 1927. Citado na página 116.
- HEISENBERG, W. *The uncertainty principle*. 1927. Disponível em: <<https://plato.stanford.edu/entries/qt-uncertainty/>>. Citado na página 116.
- HEISENBERG, W. *The Physical Principles of the Quantum Theory*. [S.l.]: Dover Dover Publications, 1949. Citado 2 vezes nas páginas 95 e 215.
- HENNESSY, J. L.; PATTERSON, D. A. *Arquitetura de Computadores - Uma Abordagem Quantitativa*. 4 ed.. ed. [S.l.]: Elsevier Editora Ltda., 2008. Citado na página 214.
- HERMANN, A. *Lexikon - Geschichte der Physik A-Z*. [S.l.]: Aulis-Verlag & Co KG Deubner, 1978. Citado na página 2.
- HEWITT, P. G. *Fisica Conceitual*. [S.l.: s.n.], 2015. 582-610 p. Citado na página 41.
- HUGHES R., e. a. *A quantum information science and technology roadmap - part 1*. 2010. Disponível em: <<http://qist.lanl.gov/acessadoemMaiode2010eOutubrode2017>>. Citado 2 vezes nas páginas viii e 242.
- HUGHES, R. J.; WILLIAMS, C. P. Quantum computing: the final frontier? *IEEE Intelligent Systems*, v. 15, 2000. Citado na página 289.
- ISAILOVIC, N. e. a. Data path and control for quantum wires. *ACM Transactions on Architecture and Code Optimization (TACO)*, v. 1, n. 1, p. 34–61, 2004. Citado 3 vezes nas páginas viii, 235 e 236.

JUNIOR, J. S. d. S. *O que é antimateria?* 2018. Acesso em: 27, Maio. Disponível em: <<https://brasilecola.uol.com.br/o-que-e/fisica/o-que-e-antimateria.htm>>. Citado na página 55.

KITAEV, A. Y. Quantum computations: algorithms and error correction. *Uspekhi Mat*, v. 52, n. 6, p. 53–112, 1997. Disponível em: <<https://iopscience.iop.org/article/10.1070/RM1997v052n06ABEH002155/meta>>. Citado na página 244.

KOIRAN, P.; NESME, V.; PORTIER, N. A quantum lower bound for the query complexity of simon's problem. *Proc. ICALP*, v. 3580, p. 1287–1298, 2005. Retrieved 2011-06-06. Citado na página 264.

KOIRAN, P.; NESME, V.; PORTIER, N. The quantum query complexity of the abelian hidden subgroup problem. *Theoretical Computer Science*, v. 380, n. 1-2, p. 115–126, 2007. Citado na página 265.

KOWADA, L. A. B. *Comparacao entre os principais protocolos para combinacao de chaves criptograficas quanticas*. mestrado, 1999. Citado 2 vezes nas páginas 271 e 272.

KOWADA, L. A. B. *Construcao de Algoritmos Reversibleis e Quanticos*. Tese (Tese de Doutorado), 2006. Citado na página 253.

LALOE, F. *Do We Really Understand Quantum Mechanics*. [S.l.: s.n.], 2012. ISBN 978-1-107-02501-1. Citado na página 39.

LEWIS, G. N. *The origin of the word "photon"*. 1926. Disponível em: <<http://www.nobeliefs.com/photon.htm>>. Citado na página 56.

LO, S.; POPESCU. *Introduction to Quantum Computation and Information*. 1998. Pp. 81-83. Citado na página 293.

MACHADO, S. R. *Implementacao da Transformada de Fourier Quantica em Nucleos Quadrupolares*. Dissertação (Mestrado), 2008. Disponível em: <[http://cbpfindex.cbpf.br/publication\\_pdfs/Tese%20Suenne.2011\\_02\\_02\\_14\\_36\\_53.pdf](http://cbpfindex.cbpf.br/publication_pdfs/Tese%20Suenne.2011_02_02_14_36_53.pdf)>. Citado na página 250.

MATIELLO, F. et al. Decifrando a computacao quantica. *Cadernos de Física da UEFS*, 2012. Disponível em: <<https://homepages.dcc.ufmg.br/~joaofnc/artigos/Computacao%20Quantica/Fundamentos/DECIFRANDO%20A%20COMPUTACAO%20QUANTICA.pdf>>. Citado 2 vezes nas páginas 184 e 187.

MAXWELL, J. C. *A Treatise on Electricity and Magnetism: Unabridged*. 3rd edition. ed. [S.l.]: Dover Publications, 1954. v. 2 Volumes. Citado na página 215.

MILIES, F. C. P.; COELHO, S. P. *Nmeros, uma introdução a Matemática*. [S.l.] : Editora da Universidade de São Paulo, 1998. Citado na página 259.

MOLGORA, A. B. d. P. *Uma implementacao do metodo das curvas elipticas para fatoracao de numeros inteiros*. Dissertação (Dissertacao de Mestrado), 2013. Disponível em: <<https://www.cbc.ufms.br>>. Citado na página 257.

- MOORE, G. E. Cramming more components onto integrated circuits. *Electronics*, 1965. Citado na página 214.
- MOSCA, M. *Quantum Algorithms*. 2008. Disponível em: <<https://arxiv.org/abs/0808.0369>>. Citado 3 vezes nas páginas 181, 244 e 245.
- NEWTON, I. *The Principia - Mathematical Principles of Natural Philosophy - A new translation by Cohen, I. B. and Whitman*. [S.l.]: A. University of California Press, 1999. Citado 2 vezes nas páginas 94 e 215.
- NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. [S.l.]: Cambridge University Press, 2000. Citado 8 vezes nas páginas 159, 180, 181, 214, 223, 232, 237 e 241.
- NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. [S.l.]: Cambridge University Press, 2002. Citado na página 250.
- NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. 10th anniversary edition. ed. [S.l.]: Cambridge University Cambridge University Press University Cambridge Cambridge University Press, 2010. Citado 3 vezes nas páginas 29, 183 e 299.
- NOVAES, M.; STUDART, N. *Mecânica Quântica Básica*. [S.l.: s.n.], 2016. (Serie MNPEF). Citado na página 300.
- ODEDOYIN. A quantum cryptography protocol for access control in big data. *International Journal on Cryptography and Information Security (IJCIS)*, v. 8, n. 2, p. 1–12, 2018. Citado 2 vezes nas páginas 291 e 292.
- OLIVEIRA, A. C.; PORTUGAL, R. *Introdução a Computação Quântica*. 2008. Disponível em: <[https://www.lncc.br/pdf\\_consultar.php?idt\\_arquivo=2445&mostrar=1](https://www.lncc.br/pdf_consultar.php?idt_arquivo=2445&mostrar=1)>. Citado 2 vezes nas páginas 186 e 238.
- OMER, B. *Quantum Programming in QCL*. Master Thesis, 2000. Citado 2 vezes nas páginas 223 e 232.
- OMER, B. *Structured Quantum Programming*. Doctorate Thesis, 2009. University of Technology. Disponível em: <<http://tph.tuwien.ac.at/~oemer/doc/structqprog.pdf>>. Citado 2 vezes nas páginas 223 e 293.
- OSKIN, M.; CHONG, F. T.; CHUANG, I. L. A practical architecture for reliable quantum computers. *IEEE Computer*, v. 35, n. 1, p. 79–87, 2002. Citado 4 vezes nas páginas viii, 238, 239 e 240.
- PIRES, A. S. T. C.; CARVALHO, R. P. de. *Por Dentro do Atomo - Física de Partículas para Leigos*. [S.l.: s.n.], 2014. ISBN 97885578611767. Citado 3 vezes nas páginas 46, 55 e 56.
- PIVETTA, M. *A Onda dos Qubits - Discórdia Quântica*. 2012. Disponível em: <>. Citado 3 vezes nas páginas 190, 194 e 195.
- PIZA, A. F. R. T. *Mecânica Quântica*. [S.l.]: EDUSP, 2003. Citado na página 184.

- POPPER, K. R. *The Logic of Scientific Discovery*. [S.l.: s.n.], 1959. First published in 1935. Citado na página 208.
- PORTUGAL, R. et al. *Uma Introducao a Computacao Quantica*. Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC), 2004. Notas em Matemática Aplicada 8. 62 p. Disponível em: <[http://www.sbmac.org.br/boletim/pdf\\_2004/livro\\_08\\_2004.pdf](http://www.sbmac.org.br/boletim/pdf_2004/livro_08_2004.pdf)>. Citado 2 vezes nas páginas 185 e 186.
- PRIZE, N. *The Nobel Prize in Physics 1918*. 2014. Disponível em: <[https://www.nobelprize.org/nobel\\_prizes/physics/laureates/1918/](https://www.nobelprize.org/nobel_prizes/physics/laureates/1918/)>. Citado na página 33.
- RABIN, M. O. Probabilistic algorithm for testing primality. *J. Number Theory*, v. 12, n. 1, p. 128–138, 1980. Citado na página 257.
- RAE, A. *Quantum Physics - Illusion or Reality?* [S.l.]: Cambridge University Press, 1986. Citado na página 216.
- RAE, A. *Quantum Physics: Illusion or reality?* Second edition. [S.l.]: Cambridge University Press, 1986–2004. ISBN ISBN-13: 978-1107604643. Citado na página 95.
- RIEFFEL, E.; POLAK, W. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, v. 32, n. 3, p. 300–335, 2000. Disponível em: <<https://core.ac.uk/download/pdf/25245217.pdf>>. Citado 5 vezes nas páginas 110, 111, 114, 186 e 187.
- RIGOLIN, G.; RIEZNIK, A. Introducao a criptografia quantica. *Revista Brasileira de Ensino de Fisica*, v. 27, n. 4, p. 517–526, 2005. Citado 8 vezes nas páginas 272, 274, 282, 283, 284, 285, 289 e 290.
- RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, v. 21, n. 2, p. 120–126, 1978. Citado na página 257.
- ROVELLI, C. *Sete Breves Licoes de Fisica*. [S.l.]: Editora Objetiva, 2015. 96 p. Citado 2 vezes nas páginas 46 e 47.
- RYDBERG, J. *Formula de Rydberg*. 1888. Disponível em: <[https://pt.wikipedia.org/wiki/Formula\\_de\\_Rydberg](https://pt.wikipedia.org/wiki/Formula_de_Rydberg)>. Citado na página 18.
- SAKURAI, J. J. *Modern Quantum Mechanics*. Revised edition. [S.l.]: Addison Wesley, 1994. Citado na página 184.
- SANTOS, J. Matrizes reais simetricas e matrizes hermitianas: Definicoes e propriedades. 2016. Universidade Federal de Uberlândia (UFU). Disponível em: <<https://www.researchgate.net/publication/305432308>>. Citado 2 vezes nas páginas 163 e 164.
- SCOTT, A. *Quantum Computing since Democritus*. [S.l.]: Cambridge University Press, 2013. 127 p. ISBN 978-0521199568. Citado na página 273.
- SHOR, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. 1994. Citado 2 vezes nas páginas 181 e 257.
- SHOR, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. *IEEE Comput. Society Press, CA*, p. 124–134, 1994. Citado 2 vezes nas páginas 181 e 257.

SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput.*, v. 26, p. 28, 1997. Disponível em: <<https://arxiv.org/abs/quant-ph/9508027>>. Citado na página 257.

SILVA, M. K. de C. *Computacao Quantica: o algoritmo de fatoracao de Shor*. 2004. Disponível em: <<https://bcc.ime.usp.br/tccs/2004/magal/mac499-monografia.pdf>>. Citado 3 vezes nas páginas 257, 259 e 262.

SIMON, D. R. On the power of quantum computation. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, p. 116–123, 1994. Retrieved 2011-06-06. Citado na página 264.

SINGH, S. *The Code Book: The science of secrecy from ancient egypt to quantum cryptography*. First anchor books edition. [S.l.: s.n.], 2000. Citado 2 vezes nas páginas 272 e 274.

SOLOVAY, R.; STRASSEN, V. A fast monte-carlo test for primality. p. 84–85, 1977. Citado na página 180.

STEIN, J. D. *Como A Matematica Explica O Mundo*. [S.l.]: Campus-Elsevier, 2008. ISBN 9788535229455. Citado 20 vezes nas páginas 30, 46, 57, 60, 61, 64, 65, 67, 72, 73, 74, 76, 78, 79, 80, 85, 86, 88, 93 e 95.

STIX, G. (Ed.). *Best-kept secrets*. 2005. Citado 2 vezes nas páginas 292 e 293.

SULZBACH, J. A. *Analise de Viabilidade de Criptografia Quantica*. Trabalho de conclusÃ£o de curso, 2003. Citado na página 292.

SVOZIL, K. Quantum algorithmic information theory. n. 2, p. 311–346, 1996. Citado na página 180.

TAMASHIRO, C. H. *Uma analise de protocolos de roteamento anonimo para redes sem fio ad hoc moveis*. Dissertacao (mestrado), 2007. Orientador: Joao Bosco M. Sobral. Disponível em: <<https://repositorio.ufsc.br/handle/123456789/90334>>. Citado na página 272.

TERADA, R. *Seguranca de Dados - Criptografia Em Redes de Computador*. [S.l.]: Editora Blucher, 2008. Citado na página 254.

TREFETHEN, L. N.; BAU, D. *Numerical Linear Algebra*. [S.l.]: Society for Industrial and Applied Mathematics (SIAM), 1997. Citado 3 vezes nas páginas 151, 170 e 171.

TURING, A. M. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, v. 2, n. 442, p. 230–265, 1936. Disponível em: <[https://www.cs.virginia.edu/~robins/Turing\\_Paper\\_1936.pdf](https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf)>. Citado na página 206.

WIESNER, S. Conjugate coding. *SIGACT*, v. 3, n. 1, p. 78–88, 1983. ISSN 0163-5700. Citado na página 272.

WIKIPEDIA. *History of quantum mechanics*. 1999. Disponível em: <[https://en.wikipedia.org/wiki/History\\_of\\_quantum\\_mechanics](https://en.wikipedia.org/wiki/History_of_quantum_mechanics)>. Citado na página 30.

WOLF, S.; WULLSCHLEGER, J. *Oblivious transfer and quantum non-locality*. 2005. Citado na página 291.

WOOTTERS, W. K.; ZUREK, W. H. *Nature*. 1982. 299, 802. Citado na página 285.

WORLD, P. *Max Planck: the reluctant revolutionary*. 2000. Disponível em: <<http://physicsworld.com/cws/article/print/2000/dec/01/max-planck-the-reluctant-revolutionary>>. Citado na página 32.



Este texto foi composto em Minion Pro, de Robert Slimbach, e Myriad Pro, de Robert Slimbach e Carol Twombly.

Este texto foi composto em fontes EBGaramond  
(<http://www.ctan.org/tex-archive/fonts/ebgaramond>).







SÉRIE PENSAMENTO MATEMÁTICO @ CIÊNCIA DA COMPUTAÇÃO

# Volume III: Computação Quântica: Aspectos Físicos e Matemáticos - Uma Abordagem Algébrica

O presente volume foi idealizado no sentido de mostrar como as raízes da Computação Quântica, a Física e a abordagem algébrica da Matemática, influíram no desenvolvimento desta ciência. Os grandes cientistas, da Física e da Matemática, avançaram no tempo, construindo a ciência que norteia e faz surgir o computador quântico. A evolução vem ocorrendo, promovida por mentes geniais, de físicos, matemáticos e lógicos que, também, construíram a abordagem lógica para a computação quântica. Cada um deles baseando-se no trabalho dos que os antecederam. A partir de problemas surgidos no início de século XX, pela limitação da Física clássica, o texto aqui apresentado reúne fatos e ideias marcantes que construíram a história fascinante da Teoria Quântica, com personagens importantes da Física, da Matemática e aqueles que pensaram na viabilidade de construção do computador quântico. Assim, chegou-se aos circuitos quânticos e aos sistemas quânticos que sustentam a Computação Quântica.

Este livro pretende servir de material inicial de apoio às disciplinas de Computação Quântica, em cursos de graduação futuros, e seu texto, seguindo o mais que possível a ordem cronológica da aparição das grandes ideias, tenta mostrar ao estudante, do ponto de vista histórico, como determinados conceitos e experimentos reveladores serviram para a aparição da Computação Quântica. Este terceiro volume faz parte da Série Pensamento Matemático @ Ciência da Computação, criada no Repositório Institucional da UFSC. É uma tentativa modesta de contribuir para os que não tem, ainda, o conhecimento histórico e conceitual, sobre os fundamentos rumo à Computação Quântica.

## Sobre o autor:

João Bosco M. Sobral é Bel. em Matemática pelo Instituto de Matemática da UFRJ em 1973, M.Sc. pelo Programa de Sistemas e Computação da COPPE-UFRJ em 1977, e Dr. pelo Programa de Engenharia Elétrica da COPPE-UFRJ em 1996. Como docente durante quatro décadas na ciência da computação da UFSC, ao participar nas disciplinas em cursos de graduação e mestrado em computação, teve a oportunidade de entender e vivenciar o elo existente entre a Matemática, a Lógica, e a Ciência da Computação. Agora, tenta disseminar o que aprendeu sobre o elo fascinante destas ciências, no sentido de motivar o leitor a ficar conectado, agora, com o mundo da Computação Quântica,

Agência Brasileira do ISBN  
ISBN 978-85-902995-4-7



9 788590 299547