V Escola do CBPF – Rio de Janeiro, de 00-00 de 2004

Computação Quântica e Informação Quântica

Ivan S. Oliveira e Roberto S. Sarthour
Centro Brasileiro de Pesquisas Físicas

RESUMO

É feita uma revisão dos princípios básicos da Mecânica Quântica, com especial foco naqueles que são os mais importantes para a Computação Quântica e Informação Quântica. Chaves lógicas quânticas e sua notação circuital são introduzidas. Duas aplicações explícitas do emaranhamento são discutidas: a codificação superdensa e o teleporte. São discutidos os principais algoritmos quânticos, tanto o princípio de funcionamento de cada um deles, quanto sua representação circuital, e as principais técnicas experimentais onde a Computação Quântica tem sido implementada em pequena escala. É discutida a criptografia quântica, e a execução do protocolo quântico BB84, para a geração de uma chave criptográfica clássica segura. Finalmente, são apresentadas noções do tratamento da Computação Quântica na presença de ruído.

1 Introdução

A Mecânica Quântica (MQ) é um conjunto de regras matemáticas que servem para a construção de teorias físicas. Dado o hamiltoniano de um sistema isolado, a MQ nos ensina como calcular os observáveis físicos em qualquer instante de tempo posterior, mas ela não diz como encontrar o hamiltoniano de um sistema.

Pode-se seguramente afirmar que a MQ é a mais bem sucedida teoria em física. Desde a sua criação até os dias de hoje ela tem sido aplicada em diversos ramos, desde a física de partículas, física atômica e molecular, na astrofísica e na matéria condensada. O seu sucesso na matéria condesada tem sido particularmente impressionante, com exemplos de aplicações na estrutura dos materiais, nas propriedades de transporte de metais, isolantes, semicondutores, nos diversos tipos de ordem magnética existentes, na supercondutividade, nas propriedades ópticas da matéria, etc.

Contudo, até o início da década de 1970 os experimentos feitos para se testar os modelos e teorias construídos a partir da MQ estavam restritos a sistemas com um número imenso de constituintes, o que fazia com que os testes só pudessem ser feitos de forma indireta. Por exemplo, a explicação da MQ da supercondutividade, conhecida como teorica BCS, é espetacular, mas os experimentos com supercondutores envolvem sempre um número muito grande de transportadores de carga (pares de Cooper). Isso significa que as previsões para o comportamento de observáveis (p. ex., a corrente supercondutora ou o calor específico em função da temperatura de uma amostra) devem feitas em termos de médias estatísticas, perdendo-se as correlações mais fundamentais entre partículas individuais. A partir da década de 1970 avanços experimentais em diversas áreas permitiram que experimentos pudessem ser feitos em números cada vez menores de partículas, tornando "visíveis" os efeitos quânticos mais fundamentais.

Neste contexto se desenvolveu a Computação Quântica (CQ), talvez a mais espetacular proposta de aplicação prática da MQ. Para fins didáticos denomina-se Informação Quântica (IQ) a identificação e o estudo dos recursos quânticos utilizáveis na área da informação, e Computação Quântica a aplicação direta desses recursos em chaves lógicas, algoritmos, etc. Este curso abordará tanto elementos de CQ quanto de IQ. O quadro abaixo resume o desenvolvimento desta área desde os seus primórdios até os dias atuais.

Ano	Fato
1973	– Demonstrada a possibilidade de computação (clássica) reversível por Charles Bennett.
1982	– Proposta de computador quântico por Paul Benioff baseado no trabalho de Charles Bennett de 1973.
1984	– Charles Bennett e Gilles Brassard descobrem o protocolo de criptografia quântica BB84.
1985	– David Deutsch cria o primeiro algoritmo quântico.
1993	– Peter Shor cria o algoritmo de fatoração. Neste ano é também descoberto o teleporte quântico por Charles Bennett e colaboradores.
1994	– Lov Grover cria o algoritmo de busca.
1996	– Um grupo da IBM demonstra experimentalmente o BB84 utilizando fótons enviados por fibras comerciais de telecomunicações.
1997	– Neil Gershenfeld e Isaac Chuang descobrem os estados pseudo-puros e fazem eclodir a CQ por Ressonância Magnética Nuclear (RMN).
1998	– Este foi o ano da Computação Quântica por RMN. Implementações de várias chaves lógicas quânticas são demonstradas através dessa técnica. São demonstrados também por RMN os algoritmos de busca e de teleporte.
2001	– É demonstrado o algoritmo de Shor por RMN.
2003	– Demonstração de emaranhamento entre os spins do núcleo e de um elétron na mesma molécula combinando-se as técnicas de RMN e RPE (Ressonância Paramagnética Eletrônica).

1.1 Os Postulados da Mecânica Quântica

A MQ é construída sobre quatro postulados:

- Postulado 1 – Todo sistema físico tem a ele associado um espaço vetorial complexo chamado de espaço de Hilbert. Os elementos do espaço de Hilbert são vetores complexos $|\psi\rangle$, chamados de kets, e representam o estado físico do sistema. O complexo conjugado de um ket é chamado de bra, representado por $\langle\psi|$.

- Postulado 2 – A evolução temporal de um sistema quântico isolado, ou seja, que não interage com sua vizinhaça, se dá através de transformações unitárias:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \tag{1}$$

onde $U^\dagger U = I$, sendo I a matriz identidade. A relação do operador U com o hamiltoniano H, em qualquer instante de tempo, do sistema é:

$$U(t) = \exp\left[-\frac{i}{\hbar}\mathcal{H}t\right] \tag{2}$$

Fisicamente, transformações unitárias representam processos temporalmente reversíveis. De fato, aplicando-se $U^\dagger$ nos dois lados da Eq. 1 obtém-se

$$|\psi(0)\rangle = U(t)^\dagger|\psi(t)\rangle \tag{3}$$

Uma outra propriedade importante das transformações unitárias é a conservação do produto escalar:

$$\langle\psi(0)|U^\dagger U|\psi(0)\rangle = \langle\psi(0)|\psi(0)\rangle = \langle\psi(t)|\psi(t)\rangle \tag{4}$$

- Postulado 3 – Medidas em MQ são representadas por um conjunto de operadores de medidas $\{M_m\}$, onde índice m refere-se aos possíveis resultados da medida. A probabilidade de que o resultado m seja encontrado em uma medida feita em um sistema quântico preparado no estado $|\psi\rangle$ é dada por

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{5}$$

e o estado do sistema após a medida com resultado m será:

$$|\psi_m\rangle = \frac{M_m}{\sqrt{p(m)}}|\psi\rangle \tag{6}$$

A normalização das probabilidades, $\sum_m p(m) = 1$, a hipótese de que $\langle\psi|\psi\rangle = 1$ e a Eq. 5 implicam na relação de completitude:

$$\sum_m M_m^\dagger M_m = I \tag{7}$$

- Postulado 4 – Os elementos do espaço de Hilbert de um sistema quântico composto $A - B$ é formado pelo produto tensorial dos kets dos espaços de Hilbert dos sistemas individuais:

$$|\psi_{A-B}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \tag{8}$$

Esta regra pode ser estendida para N sub-sistemas:

$$|\psi_{A-B-\cdots-N}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes \cdots \otimes |\psi_N\rangle \tag{9}$$

Neste curso consideraremos somente espaços de Hilbert finitos com estados discretos.

1.2 Bits e q-Bits

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

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

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

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{10}$$

O conjunto $\{|0\rangle, |1\rangle\}$ forma uma base no espaço de Hilbert de duas dimensões, chamada de base computacional. No caso de um spin 1/2 representar o q-bit, identificamos $|0\rangle \equiv |\uparrow\rangle$ e $|1\rangle \equiv |\downarrow\rangle$.

O estado genérico de um q-bit é representado por

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{11}$$

onde $|a|^2 + |b|^2 = 1$. Este estado pode ser parametrizado por ângulos θ e ϕ fazendo-se $a \equiv \cos\theta/2$ e $b \equiv \exp(i\phi)\sin\theta/2$:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \tag{12}$$

Esta representação permite que o estado de um q-bit seja vizualizado como um ponto sobre a superfície de uma esfera. Tal esfera é chamada de esfera de Bloch. Pontos especiais sobre a esfera de Bloch são mostrados na tabela abaixo.

θ	ϕ	$\|\psi\rangle$	Observação
0	0	$\|0\rangle$	pólo norte da esfera de Bloch
π	0	$\|1\rangle$	pólo sul da esfera de Bloch
$\pi/2$	0	$(\|0\rangle + \|1\rangle)/\sqrt{2}$	equador sobre o eixo x
$\pi/2$	$\pi/2$	$(\|0\rangle + i\|1\rangle)/\sqrt{2}$	equador sobre o eixo y

1.3 Aplicações dos postulados

O espaço de Hilbert de 1 q-bit tem apenas duas dimensões. Um estado genérico neste espaço é dado pela Eq. 12.

As matrizes de Pauli são importantes exemplos de transformações unitárias sobre 1 q-bit:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{13}$$

Note que em todos os casos, $UU^\dagger = I$. A ação de cada uma dessas matrizes sobre um estado genérico de 1 q-bit é

$$X|\psi\rangle = a|1\rangle + b|0\rangle \tag{14}$$

$$Y|\psi\rangle = a|1\rangle - ib|0\rangle \tag{15}$$

$$Z|\psi\rangle = a|0\rangle - b|1\rangle \tag{16}$$

Uma outra operação unitária importante sobre 1 q-bit é a transformação de Hadamard:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{X + Z}{\sqrt{2}} \tag{17}$$

Note que:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{18}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{19}$$

que implicam em

$$H^2|0\rangle = |0\rangle \tag{20}$$

Considere agora o seguinte conjunto de operadores de medida de 1 q-bit:

$$M_0 \equiv |0\rangle\langle 0|; \quad M_1 \equiv |1\rangle\langle 1| \tag{21}$$

Note que M_0 e M_1 são hermitianos mas não são unitários. Isto quer dizer que o processo de medida representado por esses operadores é irreversível. Segundo o Postulado 3,

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = |a|^2; \quad p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = |b|^2 \tag{22}$$

E após a medida,

$$|\psi_0\rangle = \frac{a}{|a|}|0\rangle \quad \text{ou} \quad |\psi_1\rangle = \frac{b}{|b|}|1\rangle \tag{23}$$

Os fatores $a/|a|$ e $b/|b|$ são fase globais (não observáveis), e podem ser descartados. Estes operadores de medidas são exemplos de projetores.

O espaço de Hilbert de dois q-bits é expandido pelos vetores formados pelo produto tensorial:

$$\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} = |00\rangle, |01\rangle, |10\rangle, |11\rangle \tag{24}$$

A representação matricial de cada um desses vetores da base computacional de dois q-bits é:

$$|00\rangle \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}; \quad |01\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}; \quad |10\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}; \quad |11\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{25}$$

A representação matricial das matrizes de Pauli e do operador de Hadamard nesta base pode ser obtida pelos produtos tensoriais correspondentes com a matriz identidade 2×2:

$$O_A = O \otimes I; \quad O_B = I \otimes O \tag{26}$$

onde $O = X, Y, Z, H$. Aqui, adota-se a convenção $|AB\rangle$ para os estados do sistema composto. Essas expressões podem ser facilmente generalizadas para um número arbitrário de q-bits.

1.4 CNOT: O Não-Controlado

A única porta de dois q-bits necessária para a implementação da Computação Quântica é a porta Não-Controlado, ou $CNOT$. Nesta porta, o estado de um dos q-bits, o q-bit alvo muda se e somente se o estado do q-bit de controle for igual a 1. A matriz que representa a porta $CNOT$ com controle no primeiro q-bit (q-bit A) é dada por:

$$CNOT_A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{27}$$

É fácil verificar que $CNOT_A|00\rangle = |00\rangle$, $CNOT_A|01\rangle = |01\rangle$, $CNOT_A|10\rangle = |11\rangle$, $CNOT_A|11\rangle = |10\rangle$.

2 Misturas Estatísticas e Matriz Densidade

Em Computação Quântica e Informação Quântica freqüentemente temos de lidar com situações em que o vetor de estado do sistema não é conhecido, mas apenas um conjunto possível de vetores $\{|\psi_i\rangle\}$, que ocorrem com probabilidades $\{p_i\}$. O conjunto $\{p_i, |\psi_i\rangle\}$ é chamado de ensemble estatístico. A ferramenta matemática adequada para tratar desses casos é a matriz densidade, ρ, definida como:

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{28}$$

onde $p_i > 0$ e $\sum_i p_i = 1$. Notemos algumas propriedades importantes deste operador:

1. A matriz densidade é um operador positivo, ou seja, possui autovalores reais não-negativos. De fato, para qualquer $|\varphi\rangle$,

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle = \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \geq 0 \tag{29}$$

2. O traço de ρ é igual a 1:

$$\mathrm{Tr}(\rho) = \sum_i p_i \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1 \tag{30}$$

3. O estado será puro se e somente se $\mathrm{Tr}(\rho^2) = 1$:

$$\begin{array}{c} \rho^2 = \sum_i \sum_j p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j| = \cdots \\ = \sum_i \sum_j p_i p_j \delta_{i,j} |\psi_i\rangle\langle\psi_j| = \sum_i p_i^2 |\psi_i\rangle\langle\psi_i| \end{array} \tag{31}$$

Consequentemente,

$$\mathrm{Tr}(\rho^2) = \sum_i p_i^2 \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i^2 \leq 1 \tag{32}$$

A igualdade será satisfeita se e somente se $p_i = 0$, exceto para um índice i_0 tal que $p_{i_0} = 1$.

Qualquer operador positivo com traço igual a 1 é um operador densidade válido.

Os postulados da MQ podem ser reformulados em termos do operador densidade.

Um exemplo de operador densidade de um ensemble canônico à temperatura de equilíbrio T é:

$$\rho = \frac{e^{-\mathcal{H}_{eq}/kT}}{\mathrm{Tr}(e^{-\mathcal{H}_{eq}/kT})} \tag{33}$$

onde $\mathcal{H}_{eq}$ é o hamiltoniano de equilíbrio do sistema. Voltaremos a este operador densidade quando discutirmos a implementação da CQ por RMN.

Quando lidamos com sistemas compostos, dado o operador densidade do sistema total, os operadores densidade dos sub-sistemas podem ser obtidos através da operação de traço parcial. O traço parcial é uma soma sobre os estados de um dos subsistemas. Por exemplo, se ρ^{AB} for o operador densidade de um sistema composto $A - B$, os operadores densidade de cada subsistema será:

$$\rho^A \equiv \mathrm{Tr}_B(\rho^{AB}); \quad \rho^B \equiv \mathrm{Tr}_A(\rho^{AB}) \tag{34}$$

Estas relações são evidentes para sistemas não-emaranhados (vide abaixo) para os quais $\rho^{AB} = \rho^A \otimes \rho^B$.

3 Emaranhamento

> "O fato de um corpo poder atuar à distância sobre o outro, através do vácuo, sem a intermediação de nada é para mim um absurdo tão grande que acredito que nenhum homem com capacidade filosófica de pensamento possa aceitar" (Isaac Newton)
>
> "Quem não se chocar com a Mecânica Quântica é porque não a compreendeu" (Niels Bohr)

"Quem afirmar que entendeu a Mecânica Quântica está mentindo" (Richard Feynman)

"Mecânica Quântica: Matemática com Magia Negra" (Albert Einstein)

O Postulado 4 e o princípio da superposição de estados quânticos permitem a consideração de estados de sistemas compostos da forma

$$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{35}$$

Estados desse tipo possuem propriedades notáveis, e constiuem um tipo de recurso computacional inteiramente novo e de natureza exclusivamente quântica.

Primeiramente note que não existem estados de q-bits individuais, $|A\rangle$ e $|B\rangle$ tais que $|\psi^+\rangle = |A\rangle \otimes |B\rangle$. Ou seja, estados como o da Eq. 35 são não-fatoráveis. Podemos calcular o operador densidade associado a este estado:

$$|\psi^+\rangle\langle\psi^+| = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2} \tag{36}$$

Usando a fórmula da entropia de Von Neumann,

$$S = -\mathrm{Tr}(\rho \log_2 \rho) = -\sum_j \lambda_j \log_2 \lambda_j \tag{37}$$

onde λ_j são os autovalores de ρ, considerando $\rho = |\psi^+\rangle\langle\psi^+|$, encontraremos $S = 0$, como era de se esperar, pois $|\psi^+\rangle$ é um estado puro. No entanto, se calcularmos o traço parcial sobre os q-bits A e B encontraremos

$$\rho_A = \rho_B = \frac{I}{2} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{38}$$

Estas matrizes densidade representam sistemas com mistura estatística máxima de cada q-bit (ou seja, $p_1 = p_2 = 1/2$). Consequentemente, a entropia associada a cada um dos q-bits individuais, $S_A = S_B = 1$, é máxima! Logo, a Eq. 35 (ou 36) representa um estado de um sistema composto com entropia zero cujos componentes individuais estão em estados de entropia máxima. Estados deste tipo são chamados de estados emaranhados. Algumas vezes o estado emaranhado $|\psi^+\rangle$ é chamado de estado do gato. Existem outros três estados emaranhados possíveis de dois q-bits:

$$|\psi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\varphi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{39}$$

$$|\varphi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

É fácil verificar que o conjunto de estados $\{|\psi^\pm\rangle, |\varphi^\pm\rangle\}$ forma uma base no espaço de estados de dois q-bits, a chamada Base de Bell.

Estados emaranhados como o estado do gato apresentam correlação perfeita entre os observáveis dos q-bits individuais. Por exemplo, se calcularmos os valores esperados de X_A e X_B para $|\psi^+\rangle$ encontraremos

$$\langle\psi^+|X_A|\psi^+\rangle = \langle X_A\rangle = \frac{\langle 00| + \langle 11|}{\sqrt{2}} \cdot \frac{|10\rangle + |01\rangle}{\sqrt{2}} = 0 \tag{40}$$

O mesmo para $\langle X_B\rangle$. No entanto, se calcularmos a correlação entre X_A e X_B, ou seja, o valor esperado de $\langle X_A X_B\rangle$, encontraremos

$$\langle\psi^+|X_A X_B|\psi^+\rangle = \langle X_A X_B\rangle = \frac{\langle 00| + \langle 11|}{\sqrt{2}} \cdot \frac{|11\rangle + |00\rangle}{\sqrt{2}} = 1 \tag{41}$$

Ou seja, embora a incerteza sobre o estado individual de cada q-bit do par seja máxima, os seus spins estão perfeitamente correlacionados!

A correlação de estados emaranhados tem consequências muito profundas e importantes para a CQ. Suponha que se faça uma medida sobre o q-bit A, representada por operadores de medida $M_0^A = |0\rangle\langle 0|$ e $M_1^A = |1\rangle\langle 1|$. A probabilidade de encontrar 0 é a mesma de encontrar 1:

$$p(0) = \langle\psi^+|M_0^{A\dagger} M_0^A|\psi^+\rangle = \langle\psi^+|M_1^{A\dagger} M_1^A|\psi^+\rangle = \frac{1}{2} = p(1) \tag{42}$$

Suponha que 0 seja encontrado. O Postulado de medidas diz que o estado após a medida será:

$$|\psi_0\rangle = \frac{M_0^A|\psi^+\rangle}{\sqrt{1/2}} = |00\rangle \tag{43}$$

Ou seja, ao encontrarmos o resultado 0 para o q-bit A, o estado do q-bit B fica também determinado (igual a 0 neste exemplo), ainda que nenhuma medida tenha sido realizada sobre B! Se considerássemos medidas em uma outra base, por exemplo, $M_+^A \equiv |+\rangle\langle +|$ e $M_-^A \equiv |-\rangle\langle -|$, ao encontrarmos o estado $|+\rangle$ para o q-bit A resultaria em um estado pós-medida igual a $|++\rangle$. Fazendo o mesmo cálculo com estados não-correlacionados, por exemplo $(|00\rangle + |01\rangle)/\sqrt{2} = |0\rangle \otimes (|0\rangle + |1\rangle)/\sqrt{2}$ verifica-se facilmente que a medida em A não afeta B.

3.1 Não-Localidade e Desigualdade de Bell

A influência do resultado de uma medida em um q-bit sobre o estado de outro q-bit, ainda que localizado remotamente em relação ao primeiro é um exemplo do que se passou a chamar não-localidade. Embora estranha, não-intuitiva e ainda pouco compreendida, a não-localidade é muito útil em CQ, como se verá em duas aplicações na próxima Seção.

Esta estranha propriedade foi apontada pela primeira vez em um influente artigo de 1935 publicado por Albert Einstein, Boris Podolsky e Nathan Rose (veja bibliografia recomendada ao final). O objetivo daquele artigo era demonstrar que a MQ é uma teoria incompleta. Segundo os autores, uma teoria completa deveria contemplar o que eles definiram como elementos de realidade. Um elemento de realidade seria, ainda segundo os autores, qualquer grandeza física cujo valor pudesse ser previsto antes que uma medida fosse feita. Por exemplo, ao se fazer uma medida do observável X sobre um q-bit de um par emaranhado, ao se encontrar o resultado 0, saber-se-ia que uma medida feita sobre o outro q-bit do par resultaria também 0. Logo, o observável X é um elemento de realidade, pois o seu valor pôde ser previsto antes da medida, ser feita. No entanto, antes que a medida no primeiro q-bit seja feita, não se pode prever o resultado, mas apenas as probabilidades dos possíveis resultados. Neste sentido é que a MQ seria uma teoria incompleta para aqueles autores. O resultado entrou para a História da Física como o Paradoxo de EPR.

Em 1964 John Bell descobriu um resultado notável, capaz de decidir em um teste experimental se a não-localidade de fato existe ou não em sistemas quânticos emaranhados. O resultado é conhecido como a desigualdade de Bell. A desigualdade de Bell estabelece um limite superior para a correlação entre medidas feitas em observáveis de q-bits separados. Trata-se de um argumento puramente estatatístico, que estabelece que uma determinada grandeza S (essencialmente a correlação entre as medidas feitas nos dois q-bits) não deveria ultrapassar o valor 2, assumindo a inexistência de efeitos não-locais. A MQ previa o valor $S = 2\sqrt{2} \approx 2,83$, portanto violando a desigualdade de Bell.

Em 1982 a desigualdade de Bell foi finalmente testada em laboratório. Um grupo francês liderado por Alain Aspect utilizou fótons emaranhados produzidos pelo decaimento de um estado excitado do ^{40}Ca e demonstraram a correlação perfeita entre as polarizações dos dois fótons. Do experimento, eles extrairam o valor $S = 2,70 \pm 0,05$, muito próximo do resultado quântico ideal.

3.2 Aplicações do Emaranhamento

Estados emaranhados constituem um recurso natural para a CQ. Duas das suas aplicações mais diretas são a codificação superdensa e o teleporte.

3.2.1 *Codificação Superdensa*

A codificação superdensa é um processo pelo qual dois bits de informação clássica podem ser transportados em um único q-bit. Suponha que Alice e Bob compartilhem um q-bit cada, de um par emaranhado, no estado do gato:

$$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{44}$$

Existem dois bits de informação clássica no conjunto, em quatro seqüências possíveis: 00, 01, 10 ou 11. Suponha que Alice deseje enviar para Bob a seqüência 10. Tudo o que ela tem a fazer é aplicar o operador X no seu q-bit (digamos, o q-bit A), transformando o estado do gato em

$$|\varphi^+\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{45}$$

Após a operação, Alice envia o seu q-bit para Bob que decodifica o estado aplicando as operações $CNOT$ e depois H, seguidas de uma medida na base computacional, para descobrir a mensagem. Dessa forma, Alice enviou 2 bits de informação clássica para Bob, enviando apenas 1 q-bit de informação quântica. Qualquer uma das quatro seqüências de dois bits pode ser enviada de forma semelhante.

3.2.2 *Teleporte*

O teleporte é um processo através do qual o estado de um q-bit é transferido para outro utilizando as propriedades não-locais de estados emaranhados. Ao contrário da codificação superdensa, o teleporte não envolve a transferência de q-bits, mas apenas de estados quânticos.

Sejam 3 q-bits em um estado inicial $|ABC\rangle = |\psi 00\rangle$, onde $|\psi\rangle = a|0\rangle + b|1\rangle$. Ou seja, $|ABC\rangle = a|000\rangle + b|100\rangle$. Considere a seguinte seqüência de operações sobre este estado[1]:

$$H_B|ABC\rangle \equiv |\Psi_1\rangle = \frac{a|000\rangle + a|010\rangle + b|100\rangle + b|110\rangle}{\sqrt{2}} \tag{46}$$

$$|\Psi_2\rangle \equiv CNOT_{BC}|\Psi_1\rangle = \frac{a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle}{\sqrt{2}} \tag{47}$$

[1]Notação: H_k = operação Hadamard sobre o q-bit k. $CNOT_{kn}$ = chave CNOT aplicada em n com controle em k.

$$|\Psi_3\rangle \equiv CNOT_{AB}|\Psi_2\rangle = \frac{a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle}{\sqrt{2}} \tag{48}$$

e finalmente,

$$\begin{aligned} &|\Psi_4\rangle \equiv H_A|\Psi_3\rangle = \cdots \\ &= \tfrac{1}{2}\left[a|000\rangle + a|100\rangle a|011\rangle + a|111\rangle + b|010\rangle - b|110\rangle + b|001\rangle - b|101\rangle\right] \end{aligned} \tag{49}$$

Este vetor pode ser escrito como:

$$\begin{aligned} |\Psi_4\rangle = \tfrac{1}{2}[&|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + \cdots \\ &|10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)] \end{aligned} \tag{50}$$

Se uma medida for feita sobre os q-bits A e B neste estado, haverá apenas 25% de chance de o q-bit C colapsar no estado $a|0\rangle + b|1\rangle$, o estado original de A.

Para que o teleporte seja implementado com 100% de sucesso, é preciso que um canal de comunicação clássico seja acionado. Isto é feito da seguinte maneira: suponha que Bob esteja de posse dos q-bits A e B, e que Alice tenha o q-bit C. Bob faz a medida nos seus dois q-bits. Suponha que ele encontre 01. Isto quer dizer que ele saberá que o q-bit de Alice está em $a|1\rangle + b|0\rangle$. Para que Alice tenha o seu q-bit no estado original de A, é necessário que Bob lhe envie uma mensagem clássica (por exemplo, telefone) e diga qual foi o resultado da sua medida. Alice aplica então o operador X ao seu q-bit, transformando o estado em $a|0\rangle + b|1\rangle$. Está completo o teleporte. Note que toda a operação não envolve o conhecimento de a e b. Note também que a necessidade de acionar um canal clássico (o telefone, ou algo equivalente) torna impossível que a informação que Bob adquire com a sua medida sobre o estado do q-bit de Alice chegue instantaneamente a ela.

4 Chaves Lógicas e Circuitos Quânticos

Uma operação lógica ou até mesmo um algoritmo pode ser descrito por um diagrama denominado circuito quântico. Estes determinam quais e em que ordem as chaves lógicas são aplicadas a um ou mais q-bits de um sistema. Os circuitos quânticos são compostos de linhas e símbolos. As linhas representam os q-bits (uma linha para cada q-bit), nescessários para realizar uma determinada operação e os símbolos representam as chaves lógicas. Por sua vez, as chaves lógicas (descritas por caixas, com letras) descrevem um conjunto de operações quânticas aplicadas a um ou mais q-bits. A seguir vamos descrever algumas operações lógicas importantes e seus respectivos circuitos quânticos.

A operação $CNOT_a$ (não controlado) pode ser descrita pelo circuito quântico ilustrado na figura 1, onde o símbolo $\oplus$ representa uma soma módulo 2

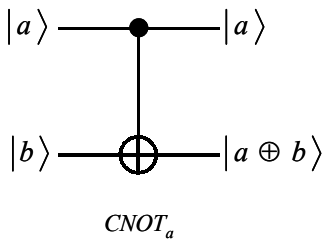

Figura 1: Circuito quântico que descreve a operação lógica $CNOT_a$.

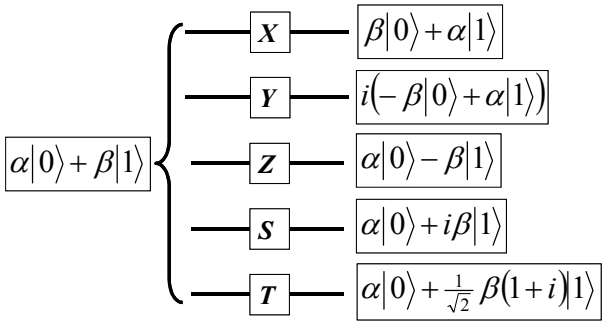

Figura 2: Circuitos quânticos que descrevem as operações lógicas de um q-bit, X, Y, Z, S (porta de fase) e T (porta $\pi/8$).

$(0 \oplus 0 = 0; 0 \oplus 1 = 1; 1 \oplus 1 = 0;)$. Esta é uma porta lógica controlada, que inverterá o q-bit b se o $a = 1$.

As operações de um q-bit são representadas por caixas, com o nome da chave lógica que deve ser implementada, como encontra-se ilustrado na figura 2, onde os símbolos representam as matrizes de Pauli (X, Y e Z), a porta de fase (S) e a porta $\pi/8$ (T).

Uma operação importante é a operação de troca (SWAP), onde os estados dos q-bits são trocados, ou seja o estado de a passa para b e vice versa, como descrito pela equação 51. Esta operação pode ser descrita pelo circuito quântico ilustrado na figura 3, e como pode ser visto, esta consiste da aplicação de três portas lógicas $CNOT$, como pode ser visto na seqüência descrita pelas equações 52.

$$SWAP\,|ab\rangle = |ba\rangle \tag{51}$$

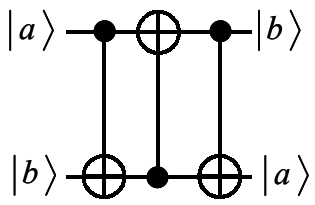

Figura 3: Circuito quântico que descreve a operação lógica U_{SWAP}, que troca os estados de dois q-bits.

$$\begin{aligned} &CNOT_a\,|a,b\rangle = |a, a\oplus b\rangle \\ &CNOT_b\,|a,a\oplus b\rangle = |a\oplus a\oplus b, a\oplus b\rangle = |b, a\oplus b\rangle \\ &CNOT_a\,|b,a\oplus b\rangle = |b, a\oplus b\oplus b\rangle = |b,a\rangle \end{aligned} \tag{52}$$

Para descrever um possível circuito para o teleporte, vamos supor que Alice e Bob se encontraram no passado e construiram um par de q-bits emaranhados no estado do gato $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, ficando cada um com um q-bit deste par. No presente momento, Alice e Bob encontram-se separados, e podem somente trocar mensagens via email. No entanto, alice quer enviar um outro q-bit ($|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$) para Bob, que nem ela conhece o estado. Ela não pode simplesmente medir o q-bit, porque ela mediria somente $|0\rangle$ ou $|1\rangle$, com probailidades $|\alpha|^2$ e $|\beta|^2$, respectivamente. A solução que Alice encontrou foi teleportar o q-bit $|\psi\rangle$ para Bob, utilizando o par de q-bits emaranhados que ambos compartilham. O circuito quântico que implementa o teleporte pode ser visto na figura 4, onde as duas linhas superiores representam os q-bits que estão com a Alice ($|\psi\rangle$ e o primeiro q-bit do par emaranhado), a linha de baixo representa o q-bit que encontra-se com Bob (o segundo q-bit do par emaranhado). Todo sistema possui então três q-bits e o seu estado inicial é descrito pela equação 53.

$$\begin{aligned} &|\Phi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \cdots \\ &= \tfrac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\right] \end{aligned} \tag{53}$$

A primeira operação do circuito é feita por Alice, que aplica a chave $CNOT_a$, ou seja inverte o segundo q-bit se o primeiro for 1 ($|a\rangle = |1\rangle$), e portanto o sistema fevolui para o estado descrito pela equação 54.

$$
\begin{aligned}
&|\Phi_1\rangle = CNOT_a\,|\Phi_0\rangle = \cdots \\
&= \tfrac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\right]
\end{aligned}
\tag{54}
$$

Em seguida, a porta Hadamard é aplicada ao primeiro q-bit, deixando o sistema no estado descrito pela equação 55.

$$
\begin{aligned}
&|\Phi_2\rangle = H_a\,|\Phi_1\rangle = \cdots \\
&= \tfrac{1}{2}\left[\alpha\,(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle) + \beta\,(|0\rangle - |1\rangle)\,(|10\rangle + |01\rangle)\right] = \cdots \\
&= \tfrac{1}{2}\left[\alpha\,(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta\,(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\right]
\end{aligned}
\tag{55}
$$

Todo processo quântico do teleporte já ocorreu, e agora devemos somente reescrever $|\Phi_2\rangle$, para que fique claro o que ocorreu no sistema. Portanto, reescrevendo 55 teremos 56:

$$
\begin{aligned}
|\Phi_2\rangle = \tfrac{1}{2}[&|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle)\cdots \\
&+ |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle)\cdots \\
&+ |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle)\cdots \\
&+ |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)]
\end{aligned}
\tag{56}
$$

Como pode ser visto da equção 56, o último q-bit, que está com Bob, encontra-se numa superposição de estados. O passo seguinte é uma medida, feita pela Alice, nos q-bits que estão com ela, que são o primeiro e o segundo. Após a medida, Alice deve enviar uma mensagem (as linhas pontilhadas na figura) para o Bob, dizendo qual foi o resultado encontrado. Bob deverá então fazer algumas operações (X^{M2} e/ou Z^{M1}), no q-bit que está com ele, que dependem do resultado da medida da Alice. Por exemplo, se ao medir os seus q-bits Alice encontrar o estado $|00\rangle$, Bob não terá que fazer nada, pois o seu q-bit já estará no estado $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Mas se o resultado da medida da Alice for $|11\rangle$, Bob terá que aplicar a porta X e depois a porta Z, para obter $|\psi\rangle$. Se o resultado da medida for $|01\rangle$ ou $|10\rangle$, Bob terá que aplicar X ou Z no seu q-bit para obter $|\psi\rangle$, respectivamente. Portanto, a função de onda final depende do resultado encontrado por Alice na sua medida, como descrito pela equação 57.

$$
\begin{aligned}
|00\rangle &\longrightarrow |\Phi_3\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \\
|01\rangle &\longrightarrow |\Phi_3\rangle = \alpha\,|1\rangle + \beta\,|0\rangle \\
|10\rangle &\longrightarrow |\Phi_3\rangle = \alpha\,|0\rangle - \beta\,|1\rangle \\
|11\rangle &\longrightarrow |\Phi_3\rangle = \alpha\,|1\rangle - \beta\,|0\rangle
\end{aligned}
\tag{57}
$$

Em computação clássica, é possível realizar qualquer operação utilizando somente a porta $NAND$ ($NOT - AND$). O mesmo acontece em computação quântica, no entanto outras portas lógicas têm que ser utilizadas. O conjunto que engloba estas portas é chamado de conjunto universal. Embora esteja fora

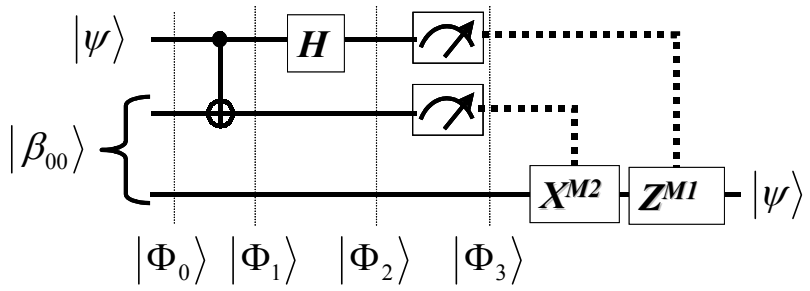

Figura 4: Circuito que implementa o teleporte. As duas linhas superiores representam os q-bits que estão com a Alice, e linha de baixo representa o q-bit que está com Bob.

do alcance deste texto, é possível demonstrar que qualquer operação quântica pode ser realizada utilizando as portas Hadamard (H), não-controlado ($CNOT$), fase (S) e $\pi/8$ (T), dentro de uma precisão arbitrária. Portanto estas portas formam um conjunto universal para computação quântica.

5 Algoritmos Quânticos

Os algoritmos quânticos são divididos em duas classes. Os de classe A são exponencialmente mais rápidos enquanto que os de classe B são somente quadraticamente mais rápidos, do que seus análogos clássicos. Até o momento existem apenas três algoritmos quânticos, que são o de Deutsch, Grover (busca) e Shor (fatoração). O algoritmo de Deutsch não tem análogo clássico e portanto não pode ser classificado, mas o algoritmo de Grover é da classe B, enquanto que o de Shor é pertence a classe A. Este último é mais rápido porque é baseado na transformada de Fourier quântica.

Como podemos perceber, existem poucos algoritmos quânticos, e há várias razões para isso. Primeira, desenvolver um algoritmo quântico ou clássico não é tarefe fácil, e a história nos ensina que é muito difícil criar bons (otimizados) algoritmos, mesmo para problemas simples. Segunda, sempre buscamos algum algoritmo que seja melhor do que seu análogo clássico. Terceira, nós vivemos num mundo clássico, ao menos é a parte que mais percebemos, e estamos mais acostumados com este do que com o intrincado mundo quântico.

5.1 O Algoritmo de Deutsch

Utilizando o algoritmo de Deutsch, é possível verificar se uma função binária é constante ($f(0) = f(1)$) ou equilibrada ($f(0) \neq f(1)$), realizando apenas uma operação com a função. Uma tentativa de analogia com alguma operação clássica seria como saber se uma moeda possui de um lado uma cara e do outro um valor (coroa), com apenas uma observação. Ou seja, é possível observar ambos os lados da moeda de uma só vez. O circuito quântico que descreve este algoritmo está ilustrado na figura 5. Neste podemos ver que a o estados de entrada dos q-bits pode ser descrito como na equação 58.

$$|\Phi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle \tag{58}$$

O passo seguinte do algoritimo é aplicar a porta Hadamard em ambos q-bits. O estado do sistema será então descrito pela equação 59.

$$\begin{array}{l} |\Phi_1\rangle = H_b H_a \, |\Phi_0\rangle = H_a \, |0\rangle \, H_b \, |1\rangle = \cdots \\ = \frac{1}{2} \left(|0\rangle + |1\rangle\right) \left(|0\rangle - |1\rangle\right) = \cdots \\ = \frac{1}{2} \left[|0\rangle \left(|0\rangle - |1\rangle\right) + |1\rangle \left(|0\rangle - |1\rangle\right)\right] \end{array} \tag{59}$$

Uma operação unitária U_f que, efetua a transformação $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ é então aplicada ao sistema. Quando aplicamos esta operação no estado de entrada $|x, y\rangle = \frac{1}{\sqrt{2}} |x\rangle \left[|0\rangle - |1\rangle\right]$ teremos o resultado descrito pela equação 60, porque $|0 \oplus f(x)\rangle = |0\rangle$ e $|1 \oplus f(x)\rangle = |1\rangle$ se $f(x) = 0$ ou $|0 \oplus f(x)\rangle = |1\rangle$ e $|1 \oplus f(x)\rangle = |0\rangle$ se $f(x) = 1$.

$$\begin{array}{l} U_f \frac{1}{\sqrt{2}} |x\rangle \left[|0\rangle - |1\rangle\right] = \frac{1}{\sqrt{2}} |x\rangle \left[|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right] = \cdots \\ = (-1)^{f(x)} \frac{1}{\sqrt{2}} |x\rangle \left[|0\rangle - |1\rangle\right] = \cdots \end{array} \tag{60}$$

Portanto, após a operação U_f o estado do sistema será o descrito pela equação 61.

$$\begin{array}{l} |\Phi_2\rangle = U_f \, |\Phi_1\rangle = \cdots \\ = \frac{1}{2} \left[(-1)^{f(0)} |0\rangle \left(|0\rangle - |1\rangle\right) + (-1)^{f(1)} |1\rangle \left(|0\rangle - |1\rangle\right)\right] \end{array} \tag{61}$$

O estado $|\Phi_2\rangle$ pode ser reescrito de modo definido pela equação 62:

$$|\Phi_2\rangle = \left\{ \begin{array}{l} \pm\frac{1}{2} \left[\left(|0\rangle + |1\rangle\right) \left(|0\rangle - |1\rangle\right)\right] \text{ Se } f(0) = f(1) \\ \pm\frac{1}{2} \left[\left(|0\rangle - |1\rangle\right) \left(|0\rangle - |1\rangle\right)\right] \text{ Se } f(0) \neq f(1) \end{array} \right\}. \tag{62}$$

O próximo passo é aplicar a chave Hadamard ao primeiro q-bit, lembrando que: $H\left(|0\rangle + |1\rangle\right) = |0\rangle$ e $H\left(|0\rangle - |1\rangle\right) = |1\rangle$, temos que o estado final do sitema será descrito pela equação 63. Finalmente, ao medirmos o estado do primeiro q-bit saberemos se a função é constante ($|0\rangle$) ou balanceada ($|1\rangle$). Resumindo, é necessário aplicar a função somente uma vez, e medir um único q-bit!

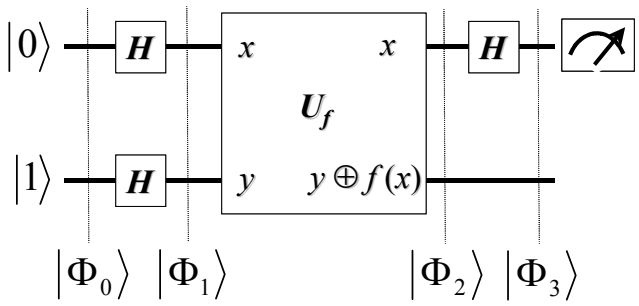

Figura 5: Representação esquemática do algoritmo de Deutsch, onde U_f é a operação da função binária $f(x)$.

$$|\Phi_3\rangle = \left\{ \begin{array}{l} \pm\frac{1}{\sqrt{2}}\left[|0\rangle\left(|0\rangle - |1\rangle\right)\right] \text{ Se } f(0) = f(1) \\ \pm\frac{1}{\sqrt{2}}\left[|1\rangle\left(|0\rangle - |1\rangle\right)\right] \text{ Se } f(0) \neq f(1) \end{array} \right\}. \tag{63}$$

5.2 O Algoritmo de Grover

Classicamente, para encontrar um item numa lista contendo N elementos, é necessário fazer em torno de $O(N)$ operações. Utilizando o algoritmo quântico de busca (Grover) podemos encontrar o item desejado fazendo somente $O(\sqrt{N})$ operações, o que coloca este algoritmo na classe B. Ainda assim, este é muito mais rápido do que seus análogos clássicos (quando N é grande).

O algoritmo de Grover realiza a busca nos indíces dos elementos ao invés de buscar os próprios elementos. O início do algoritmo é aplicar uma função - através de uma operação unitária controlada - tal que $f(x) = 1$ quando x for o item procurado e $f(x) = 0$ caso contrário. Pode-se pensar que esta operação é realizada por uma caixa preta chamada de oráculo, cuja implementação deve ser discutida particularmente para cada caso em separado. Mais precisamente, o oráculo é um operador unitário, O, cuja ação é definida pela equação 64, onde $|x\rangle$ é o q-bit de registro e $|q\rangle$ é um q-bit que é invertido se $f(x) = 1$, ou permance inalterado caso contrário.

$$O\,|x\rangle\,|q\rangle = |x\rangle\,|q \oplus f(x)\rangle \tag{64}$$

Podemos preparar o estado inicial para que este seja $|x\rangle\,|0\rangle$, e desse modo depois da aplicação do oráculo, bastará medir o estado do q-bit $|q\rangle$, para descobrirmos se x é a solução desejada. Uma aplicação interessante é aplicarmos o oráculo no estado $|x\rangle\left[|0\rangle - |1\rangle\right]/\sqrt{2}$, como encontra-se descrito pela equação

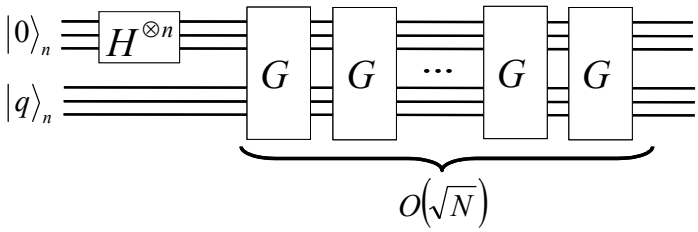

Figura 6: Circuito quântico que implementa o algoritmo de grover em um sistema com n q-bits.

65. Neste caso, a ação do oráculo foi marcar a solução invertendo a sua fase, ou seja $|x\rangle \rightarrow -|x\rangle$, se $|x\rangle$ for o índice do ítem procurado.

$$O|x\rangle \left[|0\rangle - |1\rangle\right]/\sqrt{2} = (-1)^{f(x)}|x\rangle \left[|0\rangle - |1\rangle\right]/\sqrt{2} \tag{65}$$

Como o estado do q-bit q não muda neste caso, este pode ser omitido no processo, como descrito na equação 66.

$$O|x\rangle = (-1)^{f(x)}|x\rangle \tag{66}$$

O primeiro passo do algoritmo de Grover é colocar todos os q-bits de registro do sitema no estado inicial $|0\rangle$. Em seguida aplicamos a operação Hadamard em todos estes q-bits (representada simbolicamente como: $H^{\otimes n}$). Iniciamos então um processo iterativo que aplica o operador de Grover (G) aproximadamene $O(\sqrt{N})$ vezes, como encontra-se ilustrado na figura 6.

O operador de Grover é construído a partir de quatro operações, como descrito abaixo.

$$O \rightarrow H^{\otimes n} \rightarrow 2|0\rangle\langle 0| - I \rightarrow H^{\otimes n}$$

A primeira operação é o oráculo. A segunda é aplicação da operação Hadamard em todos os q-bits. A terceira operação realiza a operação $|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle$, que inverte a fase de todos os estados exceto $|0\rangle$. Pode-se facilmente demostrar que o operador que implementa esta ação é descrito como $(2|0\rangle\langle 0| - I)$. A última operação é aplicação do Hadamard em todos os q-bits, novamente. Resumindo, o operdor de Grover pode ser descrito como na equação 67.

$$G = \left[H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}\right]O \tag{67}$$

Lembrando que a aplicação do operador de Hadamard no estado $|0\rangle$ cira uma

superposição uniforme de todos os estados ($H^{\otimes n}\left|0\right\rangle = \left|\psi\right\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\left|x\right\rangle$), podemos então reescrever o operadopr de Grover como 68:

$$G = \left[2\left|\psi\right\rangle\left\langle\psi\right| - I\right]O. \tag{68}$$

A ação do operador $\left[2\left|\psi\right\rangle\left\langle\psi\right| - I\right]$ em um estado $\sum_k \alpha_k \left|k\right\rangle$ pode ser vista na equação 69, onde $\left\langle\alpha\right\rangle \equiv \sum_k \alpha_k/N$, que o valor médio de α_k, e por esta razão esta operação é chamada de inversão em torno da média.

$$\begin{aligned}
&\left[2\left|\psi\right\rangle\left\langle\psi\right| - I\right]\sum_k \alpha_k\left|k\right\rangle = \tfrac{2}{N}\sum_k\left[\sum_{x=0}^{N-1}\sum_{x=0}^{N-1}\left|x\right\rangle\left\langle x\right|\left|k\right\rangle\alpha_k - \alpha_k\left|k\right\rangle\right] = \cdots \\
&= \tfrac{2}{N}\sum_k\left[\sum_{x=0}^{N-1}\sum_{x=0}^{N-1}\left|x\right\rangle\alpha_k\delta_{kx} - \alpha_k\left|k\right\rangle\right] = \tfrac{2}{N}\sum_k\left|k\right\rangle\sum_{k=0}^{N-1}\alpha_k - \alpha_k\left|k\right\rangle = \cdots \\
&= \sum_k\left[2\left\langle\alpha\right\rangle - \alpha_k\right]\left|k\right\rangle
\end{aligned} \tag{69}$$

O número de vezes que o operador de Grover deve ser aplicado depende do número de elementos do sistema (N) e pode ser melhor estimado, sendo igual a $\left\lfloor \pi\sqrt{N/M}/4 \right\rfloor$, onde M é número de soluções procuradas. Para $N = 4$ e $M = 1$, ou seja procurar um ítem em quatro, ($N = 2^n$; n é o número de q-bits), os operadores são descritos de acordo com a equação 70, se o índice do estado procurado for $\left|11\right\rangle$.

$$\begin{aligned}
\left[2\left|\psi\right\rangle\left\langle\psi\right| - I\right] &= \tfrac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \\
O &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \\
G = \left[2\left|\psi\right\rangle\left\langle\psi\right| - I\right]O &= \tfrac{1}{2}\begin{bmatrix} -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}
\end{aligned} \tag{70}$$

Como exemplo, descreveremos o funcionamento do algoritmo para dois q-bits ($n = 2 \Rightarrow N = 2^n = 4$ estados). O estado de entrada do algoritmo é $\left|\psi_0\right\rangle = \left|00\right\rangle$ e, a partir deste ponto, tem-se que criar uma superposição uniforme de todos os estados do sitema. Pode-se conseguir isto facilmente aplicando a chave Hadamard em cada q-bit, e com isto temos o estado

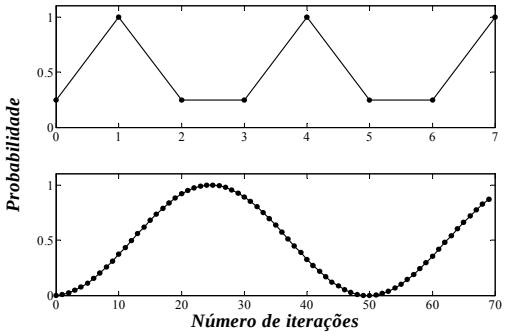

Figura 7: Probabilidade de encontrar o estado procurado versus o número de iterações do algoritmo de Grover.

$|\psi_1\rangle = \frac{1}{2}[|00\rangle + |01\rangle + |10\rangle + |11\rangle]$. Supondo que o estado procurado seja o $|11\rangle$, o oráculo deverá então inverter a fase deste estado e o sistema passará a ser descrito pela equação 71.

$$|\psi_2\rangle = O|\psi_1\rangle = \frac{1}{2}[|00\rangle + |01\rangle + |10\rangle - |11\rangle] \tag{71}$$

Em seguida, o operador $[2|\psi\rangle\langle\psi| - I]$, que faz a inversão en torno da média, deve ser aplicado ao sistema, resultando em 72:

$$G|\psi_3\rangle = |\psi_2\rangle = |11\rangle . \tag{72}$$

Para encontar outros estados, é necessário mudar somente o oráculo, de modo que este inverta a fase do estado procurado.

Na figura 7 está ilustrado o resultado da aplicação do algoritmo de Grover para dois (a) ($N = 4$) e dez (b) ($N = 1024$) q-bits. Podemos observar que o resultado da medida oscila com o número de vezes que o operador de Grover é aplicado, e portanto existe um número correto de iterações que devem ser realizadas para encontrar o elemento procurado. Este número é da rodem de $\sqrt{N}$.

5.3 O Algoritmo de Shor

Algoritmos de fatoração e determinação de ordem são necessários e importantes para decifrar códigos de sistemas criptográficos. Para fatorar classicamente um número de 1024 bits são necessários aproximadamente 100 mil anos (utilizando computadores clássicos atuais), enquanto que com o algoritmo de Shor esta

tarefa seria feita em aproximadamente $4,5$ minutos. O algoritmo de fatoração de Shor é rápido porque utiliza a transformada de fourrier quântica (TFQ), que necessita da ordem de $O(n^2)$ operações, enquanto que a sua análoga clássica, a transformada rápida de Fourier (FFT) requer algo em torno de $O(n2^n)$ operações. Também é possível estimar a fase de um estado quântico utilizando a TFQ, o que é uma aplicação extremamente importante desta operação.

A TFQ é uma transformação unitária que realiza a operação descrita pela equação 73, onde n é o número de q-bits.

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \tag{73}$$

Um modo de descobrir quais as operações lógicas necessárias para implementar a TFQ, é rescrever a segunda parte da equação acima para cada q-bit do sistema. Isto pode ser feito de modo elementar como mostra a equação 74, onde $0.j_l j_{l+1} \cdots j_m$ representa a fração binária $\frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2^{m-l+1}}$. Lembrando que podemos sempre escrever o estado $|j\rangle$ como $|j_1 j_2 \cdots j_n\rangle$ (na representação binária) e que $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$.

$$\begin{aligned}
&\tfrac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle = \cdots \\
&= \tfrac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left(2\pi ij \sum_{l=1}^{n} k_l/2^l\right) |k_1 k_2 \ldots k_n\rangle = \cdots \\
&= \tfrac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} \exp\left(2\pi ijk_l/2^l\right) |k_l\rangle = \cdots \\
&= \tfrac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} \exp\left(2\pi ijk_l/2^l\right) |k_l\rangle = \tfrac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi ij/2^l} |1\rangle\right] = \cdots \\
&= \tfrac{1}{\sqrt{2^n}} \left[\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n} |1\rangle\right)\right]
\end{aligned} \tag{74}$$

Esta última equação é muito útil, pois indica as operações que devem ser realizadas em cada q-bit para implementar a TFQ. Por exemplo, sabemos que será necessário fazer uma mudança de fase relativa em cada q-bit, e o operador (R_k) que efetua esta tarefa é definido de acordo com a equação 75.

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{75}$$

O primeiro passo do procedimento que implementa a TFQ é aplicar o operador de Hadamard para cada q-bit e depois uma série de operações lógicas controladas do tipo R_k (se o k-ésimo q-bit for igual a 1 aplica-se o operador R_k, e se o o k-ésimo q-bit for 0 não faz nada). Esta seqüência pode é descrita

na equação 76, e deve ser aplicada começando pelo primeiro q-bit. A última operação é aplicar a chave lógica de troca ($SWAP$), trocando o primerio q-bit com o último, o segundo pelo penúltimo, e assim por diante.

$$R_{n-k+1}\cdots R_3R_2H_k\left|j_1\cdots j_n\right\rangle = \frac{1}{\sqrt{2}}\left|j_1\cdots j_{k-1}\right\rangle\left[\left|0\right\rangle + e^{2\pi i 0.j_k j_{k+1}\cdots j_n}\left|1\right\rangle\right]\left|j_{k+1}\cdots j_n\right\rangle \tag{76}$$

Como exemplo aplicaremos o procedimento acima ao primeiro q-bit. O primeiro passo é aplicar o Hadamard e consequentemente teremos o estado descrito pela equação 77, porque $e^{2\pi i 0.j_1} = 1$ se $j_1 = 0$ e $e^{2\pi i 0.j_1} = -1$ se $j_1 = 1$.

$$H_1\left|j_1 j_2\cdots j_n\right\rangle = \frac{1}{\sqrt{2}}\left[\left|0\right\rangle + e^{2\pi i 0.j_1}\left|1\right\rangle\right]\left|j_2\cdots j_n\right\rangle \tag{77}$$

O próximo passo é aplicar as chaves controladas R_k, e o resultado desta operação pode ser visto nas equações 78.

$$\begin{aligned} R_2H_1\left|j_1 j_2\cdots j_n\right\rangle &= \tfrac{1}{\sqrt{2}}\left[\left|0\right\rangle + e^{2\pi i 0.j_1 j_2}\left|1\right\rangle\right]\left|j_2\cdots j_n\right\rangle \\ R_n\cdots R_2H_1\left|j_1 j_2\cdots j_n\right\rangle &= \tfrac{1}{\sqrt{2}}\left[\left|0\right\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}\left|1\right\rangle\right]\left|j_2\cdots j_n\right\rangle \end{aligned} \tag{78}$$

Esta operação deve ser repetida nos outros q-bits do sistema e ao final os estados devem ser revertidos com a operação de troca ($SWAP$), fazendo com que a TFQ seja implementada (veja equação 74).

Suponha que um operador U, cuja aplicação em dos seus autoestados tenha como resultado: $U\left|u\right\rangle = e^{2\pi i\varphi}\left|u\right\rangle$. Podemos estimar esta fase φ, utilizando a TFQ. Este algoritmo requer dois conjuntos de q-bits que são chamados de registros. O primeiro registro deve possuir um certo número de q-bits (t) e o resultado da estimativa será guardado neste registro. O segundo registro deverá ter um número de q-bits suficientes (m) para armazenar o autoestado $\left|u\right\rangle$. O estado inicial é preparado de modo que os t primeiros q-bits estejam no estado $\left|0\right\rangle$. Assim, o estado inicial fica definido como em 79.

$$\left|\psi_{ini}\right\rangle = \left|0\right\rangle_t\left|u\right\rangle \tag{79}$$

Em seguida devemos criar uma superposição uniforme de estados no primeiro registro, o que fará o sistema evoluir para o estado definido pela equação 80. Isto pode ser feito aplicando a chave Hadamard em cada q-bit do primeiro registro, e este operador possui a forma $\bigotimes_{k=1}^{t} H$.

$$\left|\psi_1\right\rangle = \frac{1}{\sqrt{2^t}}\left(\sum_{k=0}^{2^t-1}\left|k\right\rangle\right)\left|u\right\rangle \tag{80}$$

O passo seguinte é transformar o estado $|\psi_1\rangle$ em $|\psi_2\rangle$ (veja equação 81). Isto pode ser alcançado se aplicarmos as operações controladas (somente aplica o operador se o k-ésimo q-bit for igual a 1) U^{t-k} aos estados $|k\rangle|u\rangle$, tal que: $U^{t-k}|k\rangle|u\rangle = |k\rangle U^{t-k}|u\rangle = e^{2\pi i\varphi k}|k\rangle|u\rangle$.

$$|\psi_2\rangle = U^{t-k}|\psi_1\rangle = \frac{1}{\sqrt{2^t}}\left(\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle\right)|u\rangle \tag{81}$$

Neste ponto, basta aplicar a transformada inversa de Fourier quântica $TFQ^\dagger$, que pode ser obtida revertendo a seqüência de operações descrita anteriormente, no primeiro registro para obtermos $|\widetilde{\varphi}\rangle_t|u\rangle = |\varphi_1\varphi_2\cdots\varphi_t\rangle|u\rangle$. Tudo que temos que fazer agora é medir o estado do primeiro registro que teremos uma estimativa (porque o valor da fase está limitado pelo número de q-bits "t" do registro) da fase.

Agora estamos prontos para descrever o algoritmo de fatoração de Shor. Este possui algumas rotinas clássicas e apenas uma rotina quântica (etapa 4 descrita abaixo). Esta rotina é responsável por encontrar a ordem de um número, que é o menor inteiro r tal que $x^r = 1 \pmod N$, sendo a operação $y \pmod Z = y - Z \times \textit{parte inteira}\left[\frac{y}{Z}\right]$. Este procedimento é feito utilizando o algoritmo de estimativa de fase, que por sua vez utiliza a TFQ. As etapas do algoritmo de fatoração são descritas abaixo.

1. Verificar se N é par, e caso afirmativo retornar 2.
2. Determinar se $N = a^b$ para $b \geq 2$ e se aresposta for positiva retornar a.
3. Escolher um número aleatório x $(1 \leq x \leq N)$ e se $MDC(x, N) > 1$ retornar $MDC(x, N)$.
4. Encontrar a ordem r de x $(x^r = 1 \pmod N)$.
5. Se r for par e $x^{r/2} \neq -1 \pmod N$, calcule $MDC(x^{r/2}-1, N)$ e $MDC(x^{r/2}+1, N)$.Teste para saber quais são soluções não triviais e retorne-as.

A parte quântica do algoritmo de fatoração é encotrar a ordem de um número. Neste processo, dois registros também são utilizados (conjuntos com tantos q-bits quantos forem necessários), e o estado inicial do sistema deve ser preparado tal que $|\psi_{ini}\rangle = |0\rangle_t|1\rangle$. O primeiro passo é aplicar a chave Hadamard em todos os t q-bits do primeiro registro, como já foi discutido anteriormente, o que levará o sistema ao estado definido pela equação 82.

$$|\psi_1\rangle = \frac{1}{\sqrt{2^t}}\left(\sum_{k=0}^{2^t-1}|k\rangle\right)|1\rangle \tag{82}$$

O segundo passo é implementar uma operação controlada $U(x, N)$ (aplicada ao segundo registro mas controlada pelo primeiro) de modo que: $U(x, N)\,|k\rangle\,|1\rangle = |k\rangle\,\left|x^k \bmod N\right\rangle$, onde N é o número que se quer fatorar e x é um inteiro escolhido arbitrariamente tal que $1 \leq x \leq N$ (veja equação 83).

$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle\,\left|x^k \bmod N\right\rangle \tag{83}$$

Para ilustrar o procedimento, vamos fatorar o número 15. Escolhendo $x = 7$, o estado $|\psi_2\rangle$ pode ser então escrito como mostra a equação 84.

$$\begin{aligned} |\psi_2\rangle = \tfrac{1}{\sqrt{2^t}}[&|0\rangle\,|1\rangle + |1\rangle\,|7\rangle + |2\rangle\,|4\rangle + |3\rangle\,|13\rangle + \cdots \\ &+ |4\rangle\,|1\rangle + |5\rangle\,|7\rangle + |6\rangle\,|4\rangle + |7\rangle\,|13\rangle + \cdots] \end{aligned} \tag{84}$$

Como podemos observar, existe uma periodicidade no segundo registro, ou seja este somente pode estar em um dos estados $|1\rangle$, $|7\rangle$, $|4\rangle$ ou $|13\rangle$. Isto quer dizer que ao fazermos uma medida (projetiva) no segundo registro, encontraremos um dos quatro estados mencionados, e esta é justamente a próxima operação a ser realizada. Vamos supor que uma medida foi feita no segundo registro e que o estado encontrado foi o $|4\rangle$ (qualquer um serve), isto levaria o sistema ao estado descrito pela equação abaixo (eq. 85).

$$|\psi_3\rangle = \frac{1}{\sqrt{2^t}}[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \cdots]\,|4\rangle \tag{85}$$

O próximo passo é aplicar a $TFQ^\dagger$, que fará o sistema evoluir para o estado descrito pela equação 86, onde somente as amplitudes dos estados $|0\rangle$, $|512\rangle$, $|1024\rangle$ e $|1536\rangle$ são diferentes de zero e possuem a mesma probabilidade 25% de serem emcontrados, quando uma medida é feita no primeiro registro (Este procedimento não é muito intuitivo, mas pode ser facilmente calculado para um sistema de 11 q-bits, $N = 2048$, e o resultado encontra-se ilustrado na figura 8).

$$|\psi_4\rangle = \left[\sum_{k=1}^{N} \alpha_k\,|k\rangle\right]|4\rangle \tag{86}$$

Vamos supor que o estado encontrado após a medida do primeiro registro tenha sido o $|1536\rangle$. O próximo passo do processo que encontra a ordem é realizada através de um algoritmo clássico (frações contínuas), e o resultado é para $r = 4$ (para 1536). Finalmente, a próxima etapa do algoritmo de fatoração de Shor (também é um processo clássico) é calcular $MDC(x^{r/2} \pm 1, N)$ e como $MDC(7^{4/2}-1, 15) = MDC(48, 15) = 3$ e $MDC(7^{4/2}+1, 15) = MDC(50, 5) = 3$, temos que $15 = 3 \times 5$.

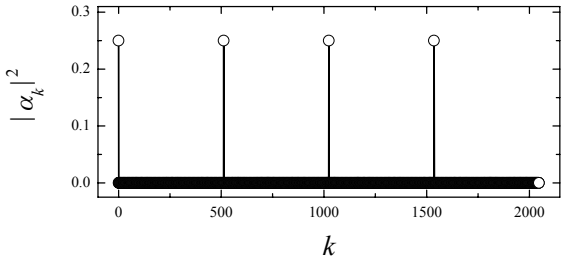

Figura 8: Amplitudes de probabilidade do estado do sistema depois da aplicação da $TFQ^{\dagger}$

6 Implementação Experimental da Computação Quântica

Exitem alguns elementos básicos e necessários para realizar computação quântica, como por exemplo os q-btis e as operações unitárias, que até aqui foram tratados como objetos matemáticos. Pode-se dizer que há quatro condições básicas que um sistema quântico deve possuir, para que uma boa implementação experimental da computação quântica seja realizada. Estas condições são:

1. Capacidade de representar de forma robusta a informação quântica.
2. Possibilidade de implementar uma família de transformações unitárias.
3. Capacidade de preparar estados iniciais (puros ou pseudo puros - $|00\ldots0\rangle$).
4. Possibilidade de medir o estado do sistema após as operações lógicas, com uma boa precisão.

No momento, existem algumas técnicas capazes de realizar computação quântica, estas são as técnicas de ótica (operações com fótons em cavidade ótica), armadilha de íons e ressonância magnética nuclear (RMN). Várias operações lógicas e circuitos quânticos já foram implementados utilizando algumas das técnicas citadas acima. Na implementção experimental da computação quântica a RMN saiu na frente e todos os algoritmos já foram implementados através da RMN. Portanto no resto desta seção, discutiremos como as operações lógicas são realizadas utilizando esta técnica, em particular.

6.1 Computação Quântica via RMN

A RMN possui várias aplicações e é utilizada por físicos, químicos, engenheiros, etc. Esta pode ser usada para caracterizar e identificar substâncias, estudar o magnetismo de materiais, controlar a qualidade de produtos, tomografia (imagens interiores), etc. Em computação quântica, a RMN é utilizada para implementar as chaves lógicas nos q-bits, que por sua vez são representados pelos spins nucleares, submetidos a um campo magnético.

Os momentos magnéticos nucleares fazem um movimento natural de precessão na presença de campos magnéticos. Os estados dos quânticos dos núcleos podem ser manipulados, irradiando os núcleos com pulsos de rádio-freqüência sintonizados na freqüência de precessão destes. Este processo é utilizado em experimentos de RMN.

Um núcleo é constituído de várias partículas (prótons e nêutrons), e a combinação dos spins destas partículas resulta em um momento angular total J. Um operador de momento angular total adimensional do núcleo é definido como: $I = J/\hbar$. O momento magnético nuclear total é proporcional a este momento ($\mu = \gamma\hbar I$), e a interação deste com um campo magnético qualquer é descrita pela equação abaixo (87).

$$\mathcal{H} = -\boldsymbol{\mu} \cdot \mathbf{B} = -\gamma\hbar \mathbf{I} \cdot \mathbf{B} \tag{87}$$

Se $\mathbf{B} = B_0\mathbf{k}$, então o hamiltoniano depende somente do operador de momento angular na direção z (I_z) e pode ser descrito como na equação 88.

$$\mathcal{H} = -\gamma\hbar B_0 I_z \Rightarrow E = -\gamma\hbar B_0 m_z \tag{88}$$

O autovalor m_z varia de $-I_z$ até I_z de uma unidade tal que $m_z = -I_z, -I_z + 1, ..., I_z - 1, I_z$. Se o núcleo possuir spin $I = 3/2$, teremos quatro níveis energia igualmente espaçados de $\Delta E = \gamma\hbar B_0$ (ver figura 9), que é o quantum de energia necessário para excitar transições.

Como $\Delta E = \hbar\omega$, temos $\omega = \gamma B_0$ que é a freqüência da radiação eletromagnética do pulso de rádio-freqüência (rf), que deverá ser aplicado para excitar transições entre os níveis de energia.

Na técnica de RMN pulsada, um campo magnético oscilante (campo de rádio-freqüência "rf") é aplicado a amostra de forma pulsada. Este campo é perpendicular ao campo estático $\mathbf{B}_0$, e sua forma pode ser descrita pela expressão 89.

$$\mathbf{B}_1(t) = B_1(\cos(\omega_z t)\mathbf{i} + \sin(\omega_z t)\mathbf{j}) \tag{89}$$

O Hamiltoniano do sistema é então dependente do tempo ($\mathcal{H}_{on}$) quando o pulso de rf está ligado, e ($\mathcal{H}_{off}$) quando desligado (ver equações 90a e 90b).

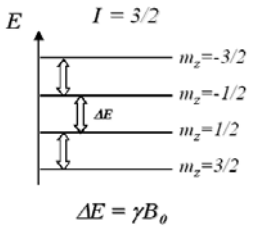

Figura 9: *Níveis de energia para spin $I = 3/2$*

$$\mathcal{H}_{on} = -\gamma\hbar\left[B_0 I_z + B_1(\cos(\omega_z t)I_x + \sin(\omega_z t)I_y)\right] \quad (90a)$$

$$\mathcal{H}_{off} = -\gamma\hbar B_0 I_z \quad (90b)$$

Este campo girante é responsável pelos pulsos de rf, e fazem com que os spins girem de determinados ângulos. Tais rotações podem ser reprsentados por transformações unitárias, descritas pelas equações 91. Estas rotações ocorrem em torno de um determinado eixo específico (por exemplo $\alpha = x$).

$$\begin{array}{c} R_\alpha(\phi) = \exp(-i\phi I_\alpha) \\ \alpha = x \text{ ou } y \text{ ou } z. \end{array} \quad (91)$$

Como o campo de rf ($\mathbf{B}_1$) é aplicado no plano xy, as rotações dos spins serão somente em torno dos eixos x ou y. O eixo de rotação é selecionado através do controle das fases dos pulsos de rf ("x" $\rightarrow 0^\circ$ "y" $\rightarrow 90^\circ$ "$-x$" $\rightarrow 180^\circ$ "$-y$" $\rightarrow 270^\circ$). O ângulo de rotação (ϕ) é deteminado pela duração e largura, do pulso de rf .

Um determinado composto pode conter alguns tipos diferentes de átomos e consequentemente de núcleos, como por exemplo o clorofórmio ($CHCl_3$). Neste composto os as ressonâncias dos núcleos de hidrogênio e carbono podem ser medidas por RMN, e estas possuem freqüências distintas. É possível escolher a freqüência de $\mathbf{B}_1$ (ω_z), com muita precisão de modo a manipular o estado quântico do núcleo de carbono sem afetar o do hidrogênio. Neste sistema em particular algumas chaves lógicas foram implementadas (ver literatura) utilizando os spins nucleares do carbono e hidrogênio como q-bits.

6.1.1 *Interação Hiperfina e Matriz Densidade*

A RMN é sensível as interações dos momentos nucleares com campos elétricos e magnéticos locais. Estas interações são chamadas de interações hiperfinas. Núcleos que possuem spin $I = 1/2$ somente possuem interação magnética, ou seja, o momento de dipolo magnético nuclear interage com algum campo magnético. No caso de dois spins (a e b) com diferentes fatores giromagnéticos (γ_a e γ_b), interagindo com um campo aplicado $\mathbf{B} = B_0\mathbf{k}$ e entre si (via uma interação de troca $\mathcal{J}_{ab}$), o Hamiltoniano do sistema é então descrito pela equação 92 (Este é exatamente o hamiltoniano que descreve o comportamento dos spins nucleares do clorofórmio, sob um campo magnético estático).

$$\mathcal{H}_{hf} = -\hbar B_0 \left[\gamma_a I_{az} + \gamma_b I_{bz}\right] + 2\hbar \mathcal{J}_{ab} I_{bz} I_{bz} \tag{92}$$

Cada tipo de spin possui uma velocidade angular que depende do campo aplicado ($\mathbf{B}_0$) e da interação de troca entre eles ($\mathcal{J}_{ab}$). Diagonalizando o Hamiltoniano Hiperfino, descrito pela equação 92, podemos obter os autovalores e autovetores deste sistema. No entanto, para calcular os espectros de RMN também é necessário conhecer a distribuição de população nos níveis de energia, e como estas populações são afetadas pela aplicação de pulsos de rf. A distribuição de população no estado de equilíbrio é dada pela matriz densidade do sistema (ver equação 93), onde Z é a função de partição, e $\beta = 1/k_B T$.

$$\rho = \frac{\exp(-\beta\mathcal{H})}{Z} \tag{93}$$

No regime de altas temperaturas, isto é $\triangle E/kT \leq 10^{-5}$, a distribuição de população do sistema descrito por 92 pode ser aproximada pela equação 94.

$$\rho \approx \frac{1}{2}\left(\mathbf{1} - \beta\mathcal{H}_{hf}\right) = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + \frac{10^{-5}}{4}\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{94}$$

Todas as mudanças em sistema quântico são refletidas na matriz densidade e a evolução no tempo destes podem ser acompanhadas de acordo com as equações 95a e 95b.

$$U(t - t_0) = \exp(-i\mathcal{H}(t - t_0)/\hbar) \tag{95a}$$

$$\rho(t) = U(t - t_0) \cdot \rho(t_0) \cdot U^{\dagger}(t - t_0) \tag{95b}$$

Como pode ser verificado facilmente utilizando as equações acima, a primeira parte da equação 94 não é afetada pelos operadores de evolução

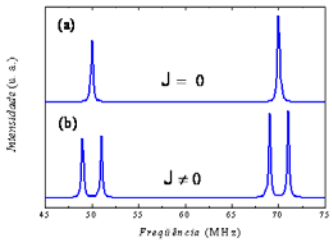

Figura 10: Espectros de RMN simulados para um sistema de 2 tipos de spins, no equlíbrio, sem (a) e com (b) interação entre eles.

$(U(t-t_0))$. Portanto, somente será observado sinal de RMN da segunda parte desta equação. Os espectros de RMN podem ser obtidos através da análise de Fourrier do sinal (uma corrente elétrica que varia no tempo) induzido na mesma bobina que aplica os pulsos de rf ($\mathbf{B}_1$). Portanto, o espectro de RMN é uma lista de freqüências versus amplitudes. As posições das linhas é dada pela separação dos níveis de energia (equação 96a), enquanto que as intensidades são dadas pela regra de ouro de Fermi ponderada pelos elementos da matriz densidade correspondente a transição e pela diferença de população (equação 96b).

$$\nu_{ij} = \frac{E_i - E_j}{h} \tag{96a}$$

$$Int_{ij} = \frac{|\langle i| V |j\rangle|^2}{\hbar^2} \left|\rho_{ij}\right| \left(\rho_{ii} - \rho_{jj}\right) \tag{96b}$$

Onde E_i são os autovalores de $\mathcal{H}_{hf}$, $\rho_{\mu\nu}$ são os elementos da matriz densidade e $V = \hbar B_1 \left(\gamma_a I_{a+} + \gamma_b I_{b+}\right)$, que é o potencial responsável por induzir transições entre os níveis de energia. Na figura 10 encontram-se ilustrados espectros de RMN do sistema descrito pelo Hamiltoniano hiperfino (equação 92), obtidos através de simulações numéricas, no estado de equlíbrio, com $\mathcal{J}_{ab} = 0$ (a) e $\mathcal{J}_{ab} = 1$ MHz (b).

6.1.2 *Criação de Estados Pseudo-Puros*

Existem algumas maneiras de ober um estado pseudo puro, por *média temporal*, *média espacial* e *rotulagem de spin*. Abaixo descreveremos com detlhes os processos de *média temporal* e *rotulagem de spin*.

O processo de média temporal, na realidade, não cria um estado pseudo puro, mas permite que operações (pode ser um algoritmo ou uma chave lógica) sobre um estado puro seja simulada fazendo uma média dos resultados obtidos realizando as mesmas operações sobre três estados quânticos distintos. O estado natural de qualquer sistema quântico é denominado estado de equilíbrio. para dois q-bits, a matriz densidade que descreve este estado em qualquer temperatura é descrita como na equação , onde a, b, c, e d são números reais e $a+b+c+d=1$.

$$\rho_0 = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix} \tag{97}$$

É sempre possível encontrar operações (P_1 e P_2) leve o sistema aos estados descritos por 98:

$$\begin{aligned} \rho_1 = P_1\rho_0 P_1^\dagger = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & b \end{bmatrix} \\ \rho_2 = P_2\rho_0 P_2^\dagger = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & c \end{bmatrix} \end{aligned} \tag{98}$$

Uma operação quântica U qualquer sobre um estado inicial faz com que este evolua segundo $\rho_\delta^t = U\rho_\delta U^\dagger$. Portanto, teremos $\rho_0^t = U\rho_0 U^\dagger$, $\rho_1^t = U\rho_1 U^\dagger$ e $\rho_2^t = U\rho_2 U^\dagger$. Fazendo uma média dos três resultados obteremos $\rho_0^t+\rho_1^t+\rho_2^t = U\left(\rho_0+\rho_1+\rho_2\right)U^\dagger$, que é descrito pela equação 99.

$$\overline{\rho} = \begin{bmatrix} 3a & 0 & 0 & 0 \\ 0 & b+c+d & 0 & 0 \\ 0 & 0 & b+c+d & 0 \\ 0 & 0 & 0 & b+c+d \end{bmatrix} \tag{99}$$

A equação acima pode reescrita lembrado que $b+c+d = 1-a$ de modo que este seja descrito pela equação 100, onde a primeira matriz respresenta um

estado puro e a segunda uma superposição uniforme (é a identidade multiplicada por um valor qualquer), que não é afetada por transformações unitárias e portanto não contribui para o sianl de RMN. A média dos espectros é o que seria obtido se operação fosse realizada em estado pseudo-puro.

$$\overline{\rho} = \begin{bmatrix} 4a-1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1-a & 0 & 0 & 0 \\ 0 & 1-a & 0 & 0 \\ 0 & 0 & 1-a & 0 \\ 0 & 0 & 0 & 1-a \end{bmatrix} \tag{100}$$

Estes três estados podem ser preparados com as sequências de pulsos descritas pelas equações 101a, 101b e 101c.

$$P_0 = \mathbf{1} \tag{101a}$$
$$P_1 = X_A \cdot \tau \cdot Y_A \cdot X_B \cdot \tau \cdot Y_B \tag{101b}$$
$$P_2 = Y_B \cdot \tau \cdot X_B \cdot Y_A \cdot \tau \cdot X_A \tag{101c}$$

Note que o primeiro estado é a própria distribuição térmica de Boltzman, equanto o segundo e terceiro são preparados com operações similares a chave lógica $CNOT$. Aqui utilizamos a notação X_A para representar um pulso de rf aplicado ao q-bit A ao longo da direção x, Y_B representa pulso de rf aplicado ao q-bit B ao longo da direção y e τ é um intervalo de tempo em o sistema evolui sem pulsos aplicados.

Um outro modo de criar um estado pseudo-puro é utilizar um spin extra para rotular os estados. Desse modo, não é necessário fazer médias como foi descrito na seção anterior. em compensação perde-se poder de computação pois um q-bit fica inutilizado para computação (este serve de rótulo para os estados pseudo puros). Neste método uma sequência de pulsos é aplicada ao sistema fazendo com que haja uma troca de populações entre os níveis de energia. Esta sequência de pulsos é a mesma que compõe a porta lógica $CNOT$.

Tomemos um sistema com dois spins como exemplo. Um $CNOT_{1-2}$ (aplicado ao spin 2 e controlado pelo spin 1, ou seja que inverte o segundo spin se o primeiro estiver para baixo) quando aplicado ao sistema que se encontra no estado inicial $|\Psi_i\rangle$ (equação 102a), resulta no estado descrito pela equação 102b.

$$|\Psi_i\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \tag{102a}$$
$$CNOT_{1-2}|\Psi_i\rangle = a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle \tag{102b}$$

Ou seja, o efeito foi de permutar as "populações" dos dois últimos estados e é exatamente este tipo de operação que podemos utilizar para criar um estado

pseudo-puro em sistemas com mais de dois tipos spins. Vamos supor que no equilíbrio um sistema com três tipos de spins possui a seguinte distribuição relativa de populações nos seus autoestados:

Estados	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
$\|\Psi_i\rangle$	6	4	4	2	4	2	2	0

Claramente, esta não é a distribuição de um estado pseudo-puro. Contudo, para esta particular distribuição de populações, é possível aplicar uma sequência de operações do tipo "$CNOT$" cujo efeito será de criar dois conjuntos de estados pseudo-puros de modo que um não interferirá no outro e vice-versa. O primeira operação que deve ser feita é aplicar um XOR_{3-1} (que inverte o primeiro spin se o terceiro estiver para baixo). Esta operação fará com que ocorra duas trocas de populações. Entre o 4° e o 8°estado e entre o 2° e 6°, contando do mais fundamental. A aplicação de um $CNOT_{2-1}$, induz uma troca de populações entre o 3° e o 7°estado e entre o 4° e 8°, como pode ser visto no quadro abaixo.

Estados	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
$\|\Psi_i\rangle$	6	4	4	2	4	2	2	0
$CNOT_{3-1}$	6	2	4	0	4	4	2	2
$CNOT_{2-1}$	6	2	2	2	4	4	4	0

Claramente a distribuição dos quatro primeiros estados, contando do mais fundamental, descreve um estado pseudo-puro. As operações lógicas podem ser realizadas somente nestes quatro estados, simplesmente selecionando as freqüências (energias) em que os pulsos de RMN são aplicados. Os quatro últimos estados também formam um estado pseudo-puro, pois possuem três níveis de energia com a mesma população. Para o caso geral de um sistema com N q-bits, o mesmo procedimento pode ser aplicado, com semelhantes operações e resultados.

Através da RMN, é possível medir a matriz densidade de desvio que pode ser definida como na equação 103a, onde ρ é matriz densidade do sistema, após algumas operações, e n é o número de q-bits.

$$\Delta\rho = \rho - \frac{\mathbf{1}}{2^n} \tag{103a}$$

Na figura encontram-se ilustrados as matrizes densidade de desvio os espectros de RMN dos 4 estados pseudo-puros para um sistema contendo 2 q-bits ($|00\rangle$, $|01\rangle$, $|10\rangle$, e $|11\rangle$). Como podemos ver, é possível identificar facilmente o estado que o sistema se encontra através da matriz densidade obtida através de experimentos de RMN.

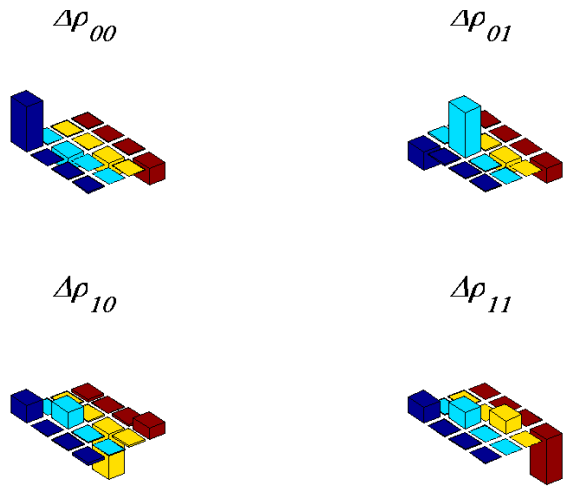

Figura 11: As matrizes densidades experimentais dos estados $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$, para um sistema com spin 3/2 (^{23}Na).

6.1.3 *Operações Lógicas via RMN*

Núcleos atômicos com spin $I = 1/2$ na presença de um campo magnético podem representar bits quânticos (q-bits). O estado com autovalor $m_z = +1/2$ representa o estado lógico "0" e o estado com autovalor $m_z = -1/2$ representa o estado "1". Utilizando a técnica de RMN é possível criar operações lógicas. Isto é feito através de pulsos de rf, que podem manipular os estados quânticos dos spins nucleares. Por exemplo a porta lógica NOT pode ser implementada com um simples pulso de rf que gire um determinado spin de 180° (ver equação 104).

$$X^2 \left|0\right\rangle = -i \left|1\right\rangle \qquad e \qquad X^2 \left|1\right\rangle = - \left|0\right\rangle \tag{104}$$

Daqui em diante, utilizaremos a notação X e Y para um pulso de $\pi/2$ ao longo dos eixos x e y, respectivamente.

Existem algumas portas lógicas que são fundamentais em computação quântica. A primeira é a porta Hadamard. Esta porta envolve somente um q-bit, e quando aplicada ao estado $|0\rangle$ cria o estado $|0\rangle + |1\rangle$.

Em um sistema de spins com $I = 1/2$ esta chave pode ser construída com pulsos de $\pi/2$ e pode ser implementadas facilmente como pode ser visto nas esquações 105a e 105b, a menos de um fator de fase global.

$$X^2 \cdot Y \left|0\right\rangle = \frac{-i}{\sqrt{2}} \left(\left|0\right\rangle + \left|1\right\rangle\right) \tag{105a}$$

$$X^2 \cdot Y \left|1\right\rangle = \frac{-i}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right) \tag{105b}$$

Para um sistema simples de 2 q-bits utilizando núcleos de spin $I = 1/2$, que interagem entre si, esta porta é construída com dois pulsos de rf, de 90°, aplicados com um intervalo de tempo específico "t", que depende da interação entre os dois spins (ver equação 106c). O operador que descreve a evolução do sistema durante este tempo está descrito pela equação 106b. O controle de fase dos pulsos é extremamente importante, pois o primeiro pulso é aplicado na direção y e o segundo na direção x. A seqüência pode ser construída da forma descrita pela equação 106a.

$$CNOT_B = Y_A \cdot \tau \cdot X_A \tag{106a}$$

$$\tau = \exp(i 2 \mathcal{J}_{ab} I_{az} I_{bz} t) \tag{106b}$$

$$t = \frac{\pi}{2\mathcal{J}_{ab}} \tag{106c}$$

O tempo "t" é o tempo necessário para que o spin A gire de um certo ângulo tal que quando o segundo pulso é aplicado este retornará para o estado

inicial, se o spin B estiver para cima ("0"), ou inverterá de 180°, se o spin B estiver para baixo ("1"). O conhecimento deste tempo é extremamente importante para implementar algoritmos quânticos, e portanto, o valor da interação entre os spins nucleares ($\mathcal{J}_{ab}$).

7 Criptografia Quântica

A criptografia é a arte da comunicação secreta. Os gregos já utilizavam a criptografia há quase 2500 anos atrás. No nosso tempo, a criptografia teve uma história particularmente fascinante durante a Segunda Grande Guerra, durante a qual os alemães criaram uma máquina para criptografar mensagens chamada de Enigma. Após um esforço imenso, e um pouco de sorte, os ingleses conseguiram construir um computador capaz de decifrar as mensagens geradas pelo Enigma. O nome dele era Colossus, e participou da sua construção ninguém menos do que o pai da computação moderna, Alan Turing.

A criptografia envolve três ingredientes básicos: as partes que desejam se comunicar em segredo, a chave criptográfica e o protocolo para codificação e decodificação da mensagem. O transmissor da mensagem deve utilizar a chave criptográfica e o protocolo de codificação para codificar a mensagem. O receptor deve fazer a operação inversa, mas para isso deve conhecer a chave criptográfica. É óbvio que se um espião quiser saber a mensagem, também deverá conhecer a chave. Assim, o problema da segurança de mensagens criptografadas se resume na segurança da distribuição de chaves entre as partes comunicantes.

Até a década de 1970 utilizava-se um sistema chamado de cripotgrafia de chave privada, no qual somente as partes comunicantes conhecem a chave secreta. Este esquema é provadamente seguro, desde que a segurança na distribuição da chave possa ser garantida. A partir dessa época foi inventado o sistema de chave pública RSA (de Rivest-Shamir-Adleman). O RSA funciona com uma chave criptográfica de duas partes: uma pública e outra secreta. A chave secreta permanece somente com o receptor da mensagem. A segurança desse sistema baseia-se na fatoração de números grandes, um problema de complexidade computacional exponencial. Fatorar um número com 2048 bits tomaria alguns milhões de anos em um computador clássico, mas desde a descoberta do algoritmo de Shor em 1993, a segurança desse sistema ficou comprometida. Em um computador quântico, um número de 2048 bits não tomaria mais do que alguns segundos para ser fatorado.

Mas o que a mecânica quântica tira com uma mão, ela dá com a outra. Em 1984 foi descoberto por Charles Bennett e Gilles Brassard um protocolo quântico para a distribuição de chaves criptográficas provadamente seguro: o BB84. Ele se baseia sobre propriedades de estados não-ortogonais que discutiremos brevemente a seguir.

7.1 Estados não-ortogonais são indistingüíveis

Considere os estados

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{e} \quad |1\rangle \tag{107}$$

Suponha que se codifique a seqüência de bits clássicos 01 como o estado de dois q-bits $|+\rangle\otimes|1\rangle$. Ao interceptar os q-bits, um hacker terá que fazer medidas para descobrir a seqüência. Se ele fizer uma medida na base de Z, ele encontrará 1 para o q-bit B, o que estará certo. No entanto, ele só terá 50 % de chance de acertar o estado do q-bit A. Se ele medir na base de X a situação permanece a mesma. A dificuldade aumenta exponencialmente com o número de q-bits na seqüência. Note que se todos os estados fossem autoestados de Z, o hacker acertaria sempre (caso escolhesse a base de Z).

7.2 Ganho de informação implica em perturbação

Suponha que duas seqüências de q-bits sejam codificadas nos estados não-ortogonais $|\psi\rangle$ e $|\varphi\rangle$. Suponha que um hacker intercepte as seqüências e tente obter informação sobre elas. Para isso ele prepara um conjunto de q-bits em um estado padrão $|s\rangle$, e os faz interagir com os q-bits de cada seqüência. Mas para que $|\psi\rangle$ e $|\varphi\rangle$ não sejam alterados (o hacker quer a informação, mas não quer ser descoberto!) essa interação deve ser unitária. A ação do hacker pode ser simbolizada como:

$$U|\psi\rangle\otimes|s\rangle = |\psi\rangle\otimes|v\rangle; \quad U|\varphi\rangle\otimes|s\rangle = |\varphi\rangle\otimes|v'\rangle \tag{108}$$

onde $|v\rangle$ e $|v'\rangle$ contém, em princípio, informação sobre $|\psi\rangle$ e $|\varphi\rangle$, respectivamente. No entanto, tomando o produto escalar, lembrando que $UU^\dagger = I$, e que $|\psi\rangle$ e $|\varphi\rangle$ são não-ortogonais, obtém-se

$$\langle v'|v\rangle = 1 \tag{109}$$

isto é, $|v\rangle \equiv |v'\rangle$. Conseqüentemente, se o hacker não pode distinguir $|v\rangle$ de $|v'\rangle$, ele não poderá distinguir $|\psi\rangle$ de $|\varphi\rangle$, e não obterá nenhuma informação sobre esses estados!

7.3 Teorema da não-clonagem

Suponha agora que o nosso frustrado hacker adote uma outra estratégia: ele tentará clonar os estados $|\psi\rangle$ e $|\varphi\rangle$ para posteriormente utilizá-los em algum ilícito. A transformação U agora deve ser tal que

$$U|\psi\rangle\otimes|s\rangle = |\psi\rangle\otimes|\psi\rangle; \quad U|\varphi\rangle\otimes|s\rangle = |\varphi\rangle\otimes|\varphi\rangle \tag{110}$$

Novamente fazendo o produto escalar, obtém-se desta vez

$$\langle\psi|\varphi\rangle^2 = \langle\psi|\varphi\rangle \tag{111}$$

Ou seja, $\langle\psi|\varphi\rangle = 0$ ou 1. Conseqüentemente, U só poderá clonar $|\psi\rangle$ e $|\varphi\rangle$ ou se eles forem idênticos, ou se forem ortogonais. Se eles forem não-ortogonais, a clonagem será impossível!

7.4 O protocolo quântico BB84

O protocolo BB84 se baseia sobre essas propriedades de estados não-ortogonais para enviar uma chave criptográfica clássica de forma segura. Os passos do protocolo são:

1. Bob seleciona duas seqüências binárias aleatórias clássicas, a e b, contendo N bits cada:

   $$a = 00010101010110101011\cdots N; \quad b = 11010101010101011010\cdots N \tag{112}$$

   A seqüência a dará origem à chave secreta. A seqüência b será utilizada como rótulo para a codificação, como descrito a seguir.

2. Bob prepara N q-bits que serão utilizados para codificar os N bits da seqüência a. A regra para a codificação é a seguinte: Se $b_i = 0$, o q-bit correspondente a a_i será codificado na base de Z, e se $b_i = 1$ a codificação será na base de X (estados $|+\rangle, |-\rangle$). Qual o elemento escolhido em uma das bases, depende do valor de a_i: para $b_i = 0$ teremos que: se $a_i = 0$, o estado do q-bit será $|0\rangle$, e se $a_i = 1$ o estado será $|1\rangle$. Para $b_i = 1$ teremos que: se $a_i = 0$, o estado do q-bit será $|+\rangle$, e se $a_i = 1$ o estado será $|-\rangle$.

   Aplicando essas regras às seqüências a e b acima, o estado dos N q-bits será:

   $$|\Psi_N\rangle = |+\rangle \otimes |+\rangle \otimes |0\rangle \otimes |-\rangle \otimes \cdots \tag{113}$$

3. Bob envia $|\Psi_N\rangle$ para Alice, mas não publica b, de modo que ela não saberá a base em que cada q-bit foi codificado. Ela prepara uma seqüência aleatória de N bits, b', e aplica a seguinte regra: se $b'_i = 0$ ela mede o q-bit correspondente na base de Z. Se $b'_i = 1$ ela mede na base de X. Como resultado da medida ela terá uma seqüência aleatória de N bits clássicos a'.

4. Após a sua medida, Alice e Bob comparam publicamente b e b', e selecionam os pares (a_i, a'_i) para os quais $b_i = b'_i$. Esses serão justamente aqueles pares que satisfazem $a_i = a'_i$. Esta é a chave secreta.

Note que em momento algum a (ou a') é tornado público. Se o estado $|\Psi_N\rangle$ for interceptado por um hacker, o teorema da não-clonagem proíbe que ele seja copiado e armazenado até a publicação de b. E se uma tentativa de medida for feita sobre o estado, isso se manifestará como uma perturbação no canal de comunicação entre Alice e Bob, que podem então abortar o protocolo e recomeçar tudo de novo.

8 Computação Quântica na Presença de Ruído

O segundo Postulado da MQ diz que a evolução de sistemas quânticos fechados se dá segundo transformações unitárias. No entanto, na maior parte das situações de interesse prático, os sistemas nunca são perfeitamente isolados, e a ação do ambiente deve ser levada em conta. O Formalismo das Operações Quânticas é uma ferramenta teórica que permite a inclusão do ambiente no problema.

De forma geral, a ação do ambiente sobre um sistema quântico resulta na modificação do seu estado ρ. Simbolicamente, esta ação é representada por uma operação quântica E, que leva ρ para ρ':

$$\rho' \equiv \mathcal{E}(\rho) \tag{114}$$

Medidas e transformações unitárias são exemplos de operações quânticas:

$$\mathcal{E}(\rho) = U\rho U^\dagger; \quad \mathcal{E}(\rho) = M_m \rho M_m^\dagger \tag{115}$$

A inclusão do ambiente no formalismo de operações quânticas é feita da seguinte forma: como o sistema combinado ambiente + sistema principal pode ser considerado isolado, ele evolui segundo transformações unitárias. Supondo que inicialmente a matriz do sistema combinado seja

$$\rho = \rho_S \otimes \rho_A \tag{116}$$

onde ρ_S é a matriz densidade do sistema principal e ρ_A do ambiente, sob uma transformação unitária U teremos:

$$\mathcal{E}(\rho) = \mathrm{Tr}_A\{U[\rho_S \otimes \rho_A]U^\dagger\} \tag{117}$$

Algumas observações importantes:

- Normalmente o sistema principal estará emaranhado com o ambiente, de forma que a hipótese $\rho_S \otimes \rho_A$ não será verdadeira. No entanto, é possível criar situações nas quais esta será uma boa aproximação.

- Como especificar U para um ambiente com infinitos graus de liberdade? Na verdade, o ambiente pode ser descrito por um espaço de Hilbert com d^2 dimensões, onde d é a dimensão do espaço de Hilbert do sistema principal.
- Não é necessário que o ambiente se inicie em uma mistura estatística; um estado puro é suficiente.

8.1 Representação do Operador-Soma

Seja $\{|e_k\rangle\}$ uma base ortonormal do espaço de estados do ambiente. Seja

$$\rho_A = |e_0\rangle\langle e_0| \tag{118}$$

o estado inicial do ambiente. Aplicando 117 vem:

$$\mathcal{E}(\rho) = \sum_k \langle e_k|U\{\rho \otimes |e_0\rangle\langle e_0|\}U^\dagger|e_k\rangle = \sum_k \langle e_k|U|e_0\rangle\rho\langle e_0|U^\dagger|e_k\rangle = \sum_k E_k\rho E_k^\dagger \tag{119}$$

onde $E_k \equiv \langle e_k|U|e_0\rangle$ são chamados de elementos de operação, e só dependem do sistema principal. Esses operadores satisfazem à relação de de completitude:

$$\sum_k E_k E_k^\dagger = I \tag{120}$$

Como exemplo considere o caso em que o sistema principal é constituído por um único q-bit, assim como o ambiente, que interagem segundo a transformação:

$$U = P_0 \otimes I + P_1 \otimes X \tag{121}$$

onde X é a matriz de Pauli usual (que atua sobre o ambiente), e $P_0 \equiv |0\rangle\langle 0|$, $P_1 \equiv |1\rangle\langle 1|$ são projetores que atuam sobre o sistema principal. Neste caso teremos dois elementos de operação: $\langle 0|U|0\rangle$ e $\langle 1|U|0\rangle$, dados por:

$$\langle 0|U|0\rangle = \langle 0|P_0 \otimes I|0\rangle + \langle 0|P_1 \otimes X|0\rangle = P_0\langle 0|0\rangle + P_1\langle 0|1\rangle = P_0 \tag{122}$$

De forma análoga se encontra $\langle 1|U|0\rangle = P_1$. Assim, a representação de operador-soma para este processo será

$$\mathcal{E}(\rho) = P_0\rho P_0^\dagger + P_1\rho P_1^\dagger = P_0\rho P_0 + P_1\rho P_1 \tag{123}$$

Note que $P_0P_0^\dagger + P_1P_1^\dagger = I$.

Alguns modelos importantes de operador-soma representando diferentes processos de ruído sobre 1 q-bit são[2]:

[2]Em cada caso, p é a probabilidade de que o bit permaneça inalterado, e $1-p$ a de que ele sofra a ação do ruído.

- Canal de inversão de bit:

$$E_0 = \sqrt{p}I, \quad E_1 = \sqrt{1-p}X \tag{124}$$

- Canal de inversão de fase:

$$E_1 = \sqrt{p}I, \quad E_1 = \sqrt{1-p}Z \tag{125}$$

- Canal de inversão de bit e de fase:

$$E_0 = \sqrt{p}I, \quad E_1 = \sqrt{1-p}Y \tag{126}$$

- Canal de despolarização:

$$E_0 = \sqrt{1-3p/4}I, \quad E_1 = \sqrt{p}/2X, \quad E_2 = \sqrt{p}/2Y, \quad E_3 = \sqrt{p}/2Z \tag{127}$$

8.2 Referências

Referências

1. M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Press, 2001).
2. D. Bouwmeester, A. Ekert and A. Zeilinger, *The Physics of Quantum Information* (Springer Verlag, 2001).
3. C.P. Williams and S.H. Clearwater, *Explorations in Quantum Computing* (Springer Verlag, 1998).
4. C.P. Slichter, *Principles of Magnetic Resonance* (3^{rd} Ed. Springer-Verlag, Berlin 1990).
5. A.P. Guimarães, *Magnetism and Magnetic Resonance in Solids* (1^{st} Ed. John Wiley & Sons, New York 1998).
6. A. Einstein, B. Podolsky and N. Rosen, *Phys. Rev.* 47 (1935) 777.
7. P. Benioff, *J. Stat. Phys.* **22** (1980) 563.

8. C. Bennett, *IBM J. Res. Dev.* **17** (1973) 525.

9. R. Feynman, *Int. J. Theor. Phys.* **21** (1982) 467.

10. D. Deutsh, *Proc. Royal Soc. London* **A400** (1985) 97.

11. P. Shor, *Proc. 35th Ann. Symp. Found. Comp. Science* (1994) 124.

12. L. Grover, *Phys. Rev. Lett.* **79** (1997) 325.

13. N. Gershenfeld and I.L. Chuang, *Science* **275** (1997) 350.

14. K. Dorai, Arvind and Anil Kumar, *Phys. Rev. A* **61** (2000) 042306-1.

15. J.A. Jones, M. Mosca, R.H. Hansen, *Nature* **393** (1998) 344.

16. G. Brassard, S.L. Braunstein and R. Cleve, *Physica D* **120** (1998) 43.

17. L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood and I.L. Chuang, *Nature* (2001) 883.

18. A.K. Khitrin and B.M. Fung, *Phys. Rev. A* **64** (2001) 032306-1.

19. C.H. Tseng, S. Somaroo, Y. Sharf, E. Knill, R. Laflamme, T.F. Havel and D.G. Cory, *Phys. Rev. A* **61** (1999) 012302.

20. Y.S. Weinstein, M.A. Pravia, E.M. Fortunato, S. Lloyd and D.G. Cory, *Phys. Rev. Lett.* **86** (2001) 1889.

21. E. Knill, R. Laflamme, R. Martinez and C.-H. Tseng, *Nature* **404** (2000)368.

22. U. Sakagushi, H. Ozawa, C. Amano and T. Fukumi, *Phys. Rev. A* **60** (1999) 1906.

23. R. S. Sarthour, E. R. deAzevedo, F. A. Bonk, E. L. G. Vidoto, T. J. Bonagamba, A. P. Guimaraes, J. C. C. Freitas and I. S. Oliveira, *Phys. Rev. A* **68** (2003) 022311-1.

24. F. A. Bonk, R. S. Sarthour, E. R. deAzevedo, J. D. Bulnes, G. L. Mantovani, J. C. C. Freitas, T. J. Bonagamba, A. P. Guimarães, and I. S. Oliveira, *Phys. Rev. A* **69** (2004) 042322-1.