Trabalho de Conclusão de Curso

Computação Quântica

Marcela Sousa Zuppini

Orientador: Pedro Aladar Tonelli

Bacharelado em Matemática Aplicada e Computacional

Instituto de Matemática e Estatística

Universidade de São Paulo

Dezembro de 2011

Resumo

Uma das razões para o campo da computação quântica ter se desenvolvido tanto nos últimos tempos e ter se tornado uma área muito ativa foi a publicação de um trabalho de Peter Shor [3], que mostrou que em um hipotético computador quântico existem algoritmos de complexidade polinomial para fatorar inteiros e para encontrar logaritmos discretos, que são soluções de uma equação exponencial sobre um grupo cíclico finito. Em computadores clássicos não existem algoritmos eficientes para esses problemas.

Este trabalho tem como objetivo apresentar a computação quântica e os conceitos matemáticos que a embasam.

Sumário

1 Introdução **1**

2 Conceitos básicos **3**

2.1 Computação clássica 3

2.2 Computação quântica 4

3 Mecânica quântica **6**

3.1 Estrutura formal 6

3.1.1 Espaço de Hilbert 6

3.1.2 Operadores lineares 9

3.1.3 Espectro de operadores lineares e medições 10

3.2 Evolução temporal do sistema quântico 12

3.3 A redução do pacote de ondas 12

4 Algoritmos quânticos **15**

4.1 Transformada de Fourier Quântica 15

4.2 Fatoração de inteiros 17

4.3 Busca desordenada 20

5 Correção de erros **24**

6 Medidas de emaranhados **29**

6.1 Emaranhados 29

6.2 Medidas de emaranhados 30

7 Conclusão **33**

Referências Bibliográficas **35**

Capítulo 1

Introdução

É possível modelar fenômenos quânticos em computadores clássicos mas extremamente difícil, devido à impossibilidade de se extrair em um computador clássico certas informações quânticas existentes em computadores quânticos, de modo que uma simulação de um computador quântico em um computador clássico não será eficiente. Por isso surgiu a ideia e, com o avanço de estudos nessa área, a necessidade de computadores quânticos.

Os estudos feitos na área da computação quântica são amplos e vão desde a criação de algoritmos simples, como algoritmos de busca, passando por pesquisas na área de criptografia, até o estudo de teletransporte.

O principal artigo estudado para a redação deste trabalho foi o *Quantum computing and entanglement for mathematicians*, publicado por Nolan R. Wallach em 2006. O artigo apresenta, inicialmente, um curso básico sobre mecânica quântica. Em seguida, ele fala sobre alguns conceitos básicos de computação clássica e quântica e apresenta alguns termos usuais da área de computação. Posteriormente, iniciam-se os estudos de alguns algoritmos quânticos, que são mais eficientes que seus análogos clássicos, seguidos de uma discussão e apresentação de um algoritmo para a correção de erros. Por fim, o artigo trata de emaranhados e da aplicação da teoria de Lie sobre a computação quântica.

A estrutura do artigo foi, em geral, mantida neste trabalho: primeiramente são apresentados alguns conceitos de computação clássica e quântica. Em seguida, é feito um estudo sobre a teoria da mecânica quântica necessária para o entendimento da computação, de forma a tentar contextualizar as estruturas da mecânica quântica dentro do campo da computação. Em seguida, são discutidos três algoritmos quânticos: a Transformada de Fourier quântica, a fatoração de inteiros e a busca numa lista desordenada. Algumas demonstrações não foram feitas por serem muito complicadas e demandarem muitos conhecimentos prévios de estruturas algébricas e resultados demonstrados em outros trabalhos. O algoritmo discutido em mais detalhes é o da busca desordenada, pois sua estrutura é mais simples do que as demais e as demonstrações exigidas nele não carecem de conhecimentos prévios. Posteriormente, é apresentada a codificação para a correção de erros, um estudo extremamente importante para o avanço da computação quântica, de forma a tornar mais próxima a possibilidade de

construção de um computador quântico. No último capítulo é feito um breve estudo sobre emaranhados e medidas de emaranhados, onde se faz uso da teoria de Lie.

Para agregar mais conhecimento sobre os tópicos discutidos, livros e outros artigos foram estudados e são tão importantes para este trabalho quanto o artigo principal, que foi seguido. Todos eles estão citados na bibliografia.

Por fim, há uma conclusão sobre os estudos feitos para a elaboração deste trabalho e um apontamento sobre os esforços atuais praticados por pesquisadores e estudiosos da computação quântica para o avanço da teoria.

Capítulo 2

Conceitos básicos

Serão apresentados neste capítulo conceitos básicos de computação clássica e quântica, como noções de bits e qubits e operações que podem ser feitas com esses elementos. Algumas estruturas matemáticas, como espaço de Hilbert, operador unitário, entre outras, serão apenas citadas neste capítulo e explicadas em detalhes no Capítulo 3.

2.1 Computação clássica

As informações armazenadas e transmitidas em computadores clássicos, como os que conhecemos, são representadas por bits, dígitos binários que podem assumir apenas dois valores, 0 e 1. Cada informação de um computador é guardada em uma cadeia de bits.

Uma cadeia com dois bits, por exemplo, pode assumir um dos quatro valores: 00, 01, 10, 11. Esses valores são representações dos inteiros 0, 1, 2 e 3 escritos na base 2. Uma cadeia com N bits poderá assumir 2^N valores, encontrados por meio da expansão na base 2 dos inteiros 0, 1, ..., N-1, que pertencem ao espaço vetorial $\mathbb{Z}_2$ x...x $\mathbb{Z}_2$.

Em geral, um computador com processador de n-bits é capaz de manipular uma cadeia de tamanho n. A maior parte dos computadores de uso pessoal possuem processadores de 32 ou 64 bits.

Um programa de computador, para simplificar, será visto como uma sequência de passos que implementa um certo conjunto de instruções, que é denominado algoritmo. O primeiro passo do algoritmo consiste em inserir na memória do computador uma sequência de bits. O passo seguinte opera na sequência que veio do passo anterior e produz uma nova sequência de bits, que poderá substituir uma sequência de algum passo anterior ou guardar a nova sequência em um novo espaço de memória. Se projetado de forma apropriada, o programa terá instruções para encerrar suas operações em algum momento e devolver uma ou mais sequências de bits, que são chamadas de variáveis de saída.

Este é o modelo de computação de John von Neumann. O fato principal deste modelo é que o computador realiza um passo de cada vez. Na verdade, os computadores que conhecemos realizam muitos passos de muitos programas (algoritmos) por vez, mas isso é

porque os computadores são um conjunto de computadores de von Neumann trabalhando simultaneamente.

Um exemplo de passo, ou operação, que um computador pode realizar é o NOT, que é um operador unitário que realiza a inversão de um valor:

a_1	$NOT\ a_1$
0	1
1	0

Outros operadores utilizados em operações na computação clássica são AND, OR e XOR.

2.2 Computação quântica

O análogo a uma cadeia de bits em um computador quântico é uma superposição de cadeias de bits, chamada de qubit. Estas superposições são representadas por coeficientes e cadeias de bits. Numa linguagem mais simplificada, as cadeias de bits são estados puros e os qubits são "combinações" desses estados, onde os coeficientes indicam o "peso" de cada estado nesta "combinação". Assim, considerando-se um espaço vetorial com 2 elementos sobre $\mathbb{C}$, por exemplo, um qubit é um elemento pertencente a este espaço descrito da seguinte maneira:

$$a\,|0\rangle + b\,|1\rangle, \qquad \text{com } |a|^2 + |b|^2 = 1,$$

onde a e b são os coeficientes e $|0\rangle$ e $|1\rangle$ são os estados puros.

A notação $|\,\rangle$ é parte de uma notação conhecida como Notação Bra-Ket e é devida a Paul Dirac. Essa notação é muito utilizada em mecânica quântica e será explicada detalhadamente no Capítulo 3. Por ora, a utilização dela é justificada pelo seguinte fato: como as cadeias de bits são sequências de valores e os coeficientes podem assumir esses valores, a notação de Dirac é usada para diferenciar estes dois elementos. Ou seja, no caso do exemplo acima, se os coeficientes a e b valessem 1 e 0, respectivamente, a notação de Dirac deixaria claro que o "peso" do estado $|0\rangle$ é 1 e que o "peso" do estado $|1\rangle$ é 0. Portanto, o qubit seria escrito como $1\,|0\rangle + 0\,|1\rangle$. Sem a notação em questão teríamos o qubit representado por $10 + 01$, que não deixa claro quem são os coeficientes e quem são os bits.

Ainda sobre o qubit descrito acima, dizemos que ele pode estar no estado $|0\rangle$ com probabilidade $|a|^2$ e no estado $|1\rangle$ com probabilidade $|b|^2$. Este é um resultado da teoria de mecânica quântica e será explicado no capítulo a seguir.

Já é a possível notar a principal diferença entre computação clássica e quântica: apesar do qubit ser composto por estados discretos (no caso do exemplo citado, $|0\rangle$ e $|1\rangle$), existem infinitas superposições possíveis para um qubit, pois os coeficientes (no caso do exemplo, a e b) podem assumir infinitos valores.

Se tivéssemos uma cadeia com 2 bits, o correspondente do espaço vetorial de qubits seria um elemento do tipo

$$u = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle, \qquad \text{com } |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1.$$

Interpretamos essa relação da seguinte maneira: o qubit u pode estar no estado $|00\rangle$ com probabilidade $|a|^2$, no estado $|01\rangle$ com probabilidade $|b|^2$, e assim por diante. O mesmo resultado é estendido para n-qubit.

As operações básicas com qubits, em um computador quântico, envolvem transformações permitidas na mecânica quântica, ou seja, operações unitárias e medições. Assim, vamos considerar que o análogo ao passo na computação clássica é uma transformação unitária num espaço de Hilbert de cadeias de bits.

Da mesma forma que um programa em um computador clássico, um programa quântico é uma sequência de passos, ou de transformações unitárias, e funciona de maneira análoga à aquele. Portanto, o programa começa com um n-qubit u_0 e faz uma sequência de transformações unitárias T_j sobre este estado. Assim, os passos são $u_1 = T_1\,u_0$, $u_2 = T_2\,u_1$, ..., $u_m = T_m\,u_{m-1}$. Um programa quântico também contém instruções de parada e, neste momento, ele deve fazer uma medição. O resultado desta medição é a variável de saída.

É possível representar um qubit u da seguinte maneira:

$$u = cos\theta|0\rangle + e^{i\varphi}sen\theta|1\rangle,$$

com $-\frac{\pi}{2} \leq \theta \leq \frac{\pi}{2}$ e $0 \leq \varphi \leq 2\pi$ [10]. A partir dessa maneira de escrever um qubit u, é possível representá-lo graficamente na esfera de Bloch, que é uma esfera de raio unitário, mostrada na figura abaixo.

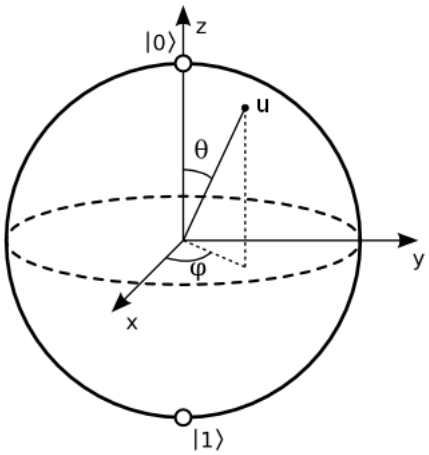

Figura 2.1: Esfera de Bloch

Capítulo 3

Mecânica quântica

A teoria quântica teve seu ponto de partida com Werner Karl Heisenberg e suas teorias foram consolidadas por Max Born e Pascual Jordan. Em paralelo, houve um processo de invenção que culminou em um realização diferente da teoria quântica, publicada em 1926 por Erwin Schrödinger. A equivalência da teoria de Heisenberg com a de Schrödinger foi provada por este último ainda em 1926.

A consolidação do esqueleto formal comum às duas teorias se deve em grande parte à Paul Dirac, que escreveu e editou algumas vezes o artigo *The Principles of Quantum Mechanics*.

A teoria da mecânica quântica ainda foi reinventada uma vez mais por Richard Feynman na década de 40, numa forma que deu início a um terceiro tipo de realização que, embora seja tecnicamente muito mais complicado que as realizações de Heisenbeg e Schrödinger, oferece novos pontos de vista sobre o assunto.

Apesar de muito estudada e desenvolvida, a teoria quântica ainda carece de alguns formalismos, como a demonstração da relação entre vários de seus elementos e o domínio mais concreto do resultado de medições realizadas ou realizáveis [2].

3.1 Estrutura formal

Este capítulo abordará os aspectos mais básicos e necessários da teoria quântica para o entendimento da computação quântica. O tratamento que será desenvolvido a seguir é suficiente apenas para o caso de espaços vetoriais de dimensão finita. No caso de espaços de dimensão infinita é necessário um tratamento usando análise funcional.

3.1.1 Espaço de Hilbert

A estrutura algébrica da mecânica quântica se baseia na álgebra linear em espaços vetoriais sobre números complexos, munidos de um produto escalar hermiteano. Estes espaços vetoriais satisfazem os mesmos axiomas de espaços vetoriais sobre $\mathbb{R}$, exceto que escalares são agora obtidos em $\mathbb{C}$.

Para descrever os vetores deste espaço, será utilizada a notação de Paul Dirac, na qual um vetor genérico é indicado pelo símbolo $|\,\rangle$. Vetores específicos aparecerão então sob a forma $|\varphi\rangle, |\psi\rangle$, etc.

Portanto, no espaço vetorial complexo estão definidas operações de soma de vetores e de produto de vetor por complexo, onde a soma e produto satisfazem as seguintes propriedades:

- Soma:
  1. associativa: $|\varphi\rangle + (|\psi_1\rangle + |\psi_2\rangle) = (|\varphi\rangle + |\psi_1\rangle) + |\psi_2\rangle$;
  2. comutativa: $|\varphi\rangle + |\psi\rangle = |\psi\rangle + |\varphi\rangle$;
  3. existência de vetor nulo: existe $|0\rangle$ tal que $|\varphi\rangle + |0\rangle = |\varphi\rangle$;
  4. existência de vetor oposto: para todo vetor $|\varphi\rangle$ existe um outro vetor $|-\varphi\rangle$ tal que $|\varphi\rangle + |-\varphi\rangle = |0\rangle$.
- Produto:
  1. associativa: $(z_1 z_2)\,|\varphi\rangle = z_1(z_2\,|\varphi\rangle)$;
  2. distributiva: $(z_1 + z_2)|\varphi\rangle = z_1\,|\varphi\rangle + z_2\,|\varphi\rangle$ e $z(|\varphi\rangle + |\psi\rangle) = z\,|\varphi\rangle + z\,|\psi\rangle$;
  3. produto pela unidade: o produto de qualquer vetor por $z = 1$ resulta no mesmo vetor, $1\,|\varphi\rangle = |\varphi\rangle$.

Como dito anteriormente, a teoria quântica é baseada em espaços vetoriais sobre $\mathbb{C}$ no qual está definido um produto escalar hermitiano.

O produto hermitiano associa a todo par de vetores $|\varphi\rangle, |\psi\rangle$ um número complexo, que será indicado pelo símbolo $\langle\varphi, \psi\rangle$ e que satisfaz os seguintes axiomas [11]:

1. $\langle\varphi, \psi\rangle = \overline{\langle\psi, \varphi\rangle}$ (a barra representa o complexo conjugado);
2. $\langle\varphi, \psi + \xi\rangle = \langle\varphi, \psi\rangle + \langle\varphi, \xi\rangle$;
3. $\langle\alpha\varphi, \psi\rangle = \alpha\langle\varphi, \psi\rangle$ e $\langle\varphi, \alpha\psi\rangle = \overline{\alpha}\langle\varphi, \psi\rangle$, onde $\alpha \in \mathbb{C}$;
4. $\langle\varphi, \psi\rangle \geq 0$, para todo φ e ψ pertencentes a E.

Da propriedade 1 resulta que o produto escalar hermitiano de um vetor consigo mesmo é um número real, que pode ser definido como o quadrado da norma desse vetor, ou seja, $||\varphi||^2 = \langle\varphi, \varphi\rangle$.

Definimos também que $|\varphi\rangle$ é perpendicular ou ortogonal a $|\psi\rangle$ se $\langle\varphi, \psi\rangle = 0$.

A última propriedade a ser comentada é que qualquer vetor deste espaço pode ser expandido em uma base de vetores $\{\Phi_n\}$, $n = 1,2,...$, mutuamente ortogonais e de norma igual a 1. Assim, um vetor $|\varphi\rangle$ pode ser escrito como

$$|\varphi\rangle = \sum_n c_n |\Phi_n\rangle,$$

onde os coeficientes c_n pertencem a $\mathbb{C}$ e podem ser expressos em termos do produto escalar, $c_n = \langle \Phi_n, \varphi \rangle$. Uma base com esta propriedade é chama de *base ortonormal*.

Uma classe importante de objetos definidos em um espaço vetorial complexo é a classe das funções lineares, com valores complexos, cujo argumento é um vetor do espaço. A notação geométrica introduzida por Dirac para esses objetos é $\langle\,|$. Assim, funções lineares específicas aparecerão sob a forma $\langle f|, \langle g|$, etc. Então, o resultado da ação da função linear $\langle f|$ sobre o vetor $|\varphi\rangle$ será um número complexo representado por $\langle f|\varphi\rangle$.

A linearidade das funções significa que, para qualquer função linear f

$$\langle f| \left(z_1|\varphi\rangle + z_2\,|\psi\rangle\right) = z_1\langle f|\varphi\rangle + z_2\langle f|\psi\rangle,$$

isto é, o número complexo que resulta da aplicação de uma função linear qualquer sobre uma combinação linear de vetores é igual à combinação linear dos números complexos que resultam da aplicação dessa função sobre cada um dos vetores separadamente.

O conjunto de funções lineares obedecem a todas as propriedades de espaços vetoriais, portanto este conjunto também é um espaço vetorial, chamado de *espaço dual* do espaço de partida.

Dirac chamou de *bras* os vetores do espaço dual e *kets* os vetores do espaço de partida, de modo que usando a notação Bra-Ket (citada no Capítulo 2) os produtos escalares aparecem representados por *brackets* (parênteses) do tipo $\langle\varphi|\psi\rangle$, que correspondem a números complexos.

Um espaço vetorial complexo, munido de um produto escalar que define, em particular, a norma dos vetores que o constituem, é chamado **espaço de Hilbert** quando dotado ainda da propriedade adicional de completude [2]. Essa propriedade significa que toda sequência de Cauchy converge para um vetor deste espaço.

Um espaço de Hilbert assim definido será então tomado como a estrutura sobre a qual pode ser desenvolvida a dinâmica da teoria quântica.

Um exemplo de espaço de Hilbert é o espaço $\mathbb{C}^n$, para n finito, munido do produto interno $\langle x, y\rangle = \sum_k \overline{x_k} y_k$.

Já no contexto de computação quântica considera-se que os qubits (superposições de bits) são os vetores de um espaço de Hilbert, cujos coeficientes associados pertencem a $\mathbb{C}$. Considere, por exemplo, o espaço de Hilbert formado por qubits de cadeias de tamanho 2, cujos estados puros são $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Neste caso, o produto interno dos estados

$$u = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle \;\; e$$

$$v = \beta_1|00\rangle + \beta_2|01\rangle + \beta_3|10\rangle + \beta_4|11\rangle$$

é definido da sequinte maneira:

$$\langle u, v\rangle = \alpha_1\beta_1|00\rangle|00\rangle + \alpha_1\beta_2|00\rangle|01\rangle + ... + \alpha_4\beta_3|11\rangle|10\rangle + \alpha_4\beta_4|11\rangle|11\rangle.$$

O produto interno assim definido satisfaz os axiomas descritos na seção anterior.

3.1.2 Operadores lineares

Vamos revisar alguns conceitos de álgebra linear referentes a operadores lineares, pois as variáveis dinâmicas dos sistemas quânticos correspondem a operadores lineares particulares do espaço de Hilbert. No caso de computadores quânticos, as operações realizadas com qubits são feitas por meio destes operadores lineares.

Um operador linear age sobre os vetores do espaço dando como resultado outros vetores do mesmo espaço, satisfazendo condições de linearidade. Ou seja, se f é um operador linear sobre o espaço E, e $|\varphi\rangle$ e $|\psi\rangle$ são vetores deste espaço, então:

- $f|\varphi\rangle$ é um vetor de E e
- $f(\alpha_1|\varphi\rangle + \alpha_2|\psi\rangle) = \alpha_1 f|\varphi\rangle + \alpha_2 f|\psi\rangle$, com α_1 e α_2 quaisquer e pertencentes a $\mathbb{C}$.

No caso de um espaço vetorial de dimensão finita, a ação de um operador linear sobre qualquer vetor do espaço estará bem definida sempre que a ação do operador sobre cada um dos vetores da base associada ao vetor em questão estiver bem definida. Isso pode não ser verdade no caso de um espaço de dimensão infinita.

A soma e o produto de operadores lineares podem ser definidos pelas relações

$$(g + h)|\varphi\rangle = g|\varphi\rangle + h|\varphi\rangle \quad \text{e} \quad (gh)|\varphi\rangle = g(h|\varphi\rangle),$$

e correspondem também a operadores lineares.

É possível associar a cada operador g outro operador $g^\dagger$, chamado **operador adjunto** de g, através da relação

$$\langle\varphi|g^\dagger|\psi\rangle = \overline{\langle\psi|g|\varphi\rangle},$$

para quaisquer vetores $|\varphi\rangle$ e $|\psi\rangle$. A representação matricial do operador adjunto $g^\dagger$ é a complexo-conjugada da transposta da matriz que representa g.

A definição de operador adjunto apresenta problemas no caso de operadores não limitados. A maneira de se contornar essa dificuldade pode ser encontrada em [2], pág. 55.

Um operador linear f é dito **hermitiano**, ou auto-adjunto, se satisfaz:

$$\langle\varphi, f\psi\rangle = \langle f\varphi, \psi\rangle \quad \text{ou} \quad f^\dagger = f, \tag{3.1}$$

para quaisquer dois vetores do espaço.

Usando a propriedade 1 de produto hermitiano, verifica-se que as matrizes que representam operadores hermitianos em bases ortonormais são sempre tais que $f_{nm} = \overline{f_{mn}}$.

Há ainda duas classes importantes de operadores lineares a serem comentadas: a dos operadores unitários e a dos operadores de projeção.

Os **operadores unitários** possuem a seguinte propriedade:

$$u^\dagger = u^{-1} \quad \text{ou} \quad u^\dagger u = u u^\dagger = \hat{1}.$$

Um operador unitário transforma uma base ortonormal em outra base ortonormal do espaço vetorial.

Dentro do contexto de computação quântica, esses operadores são tais que, dado, por exemplo, um estado

$$\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle,$$

sua evolução durante um intervalo de tempo para o estado

$$\beta_1|00\rangle + \beta_2|01\rangle + \beta_3|10\rangle + \beta_4|11\rangle$$

obedece a seguinte relação

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{bmatrix},$$

onde as matrizes que satisfazem essa relação são operadores unitários.

Exemplos de operadores unitários aparecerão nos Capítulos 4 e 5.

Já os **operadores de projeção** são identificados pelas seguintes propriedades:

$$P^\dagger = P \quad \text{e} \quad P^2 \equiv PP = P.$$

A segunda propriedade é conhecida como propriedade de *idempotência*.

Um exemplo de operador de projeção será visto na Seção 4.3.

3.1.3 Espectro de operadores lineares e medições

Será dada nesta seção uma interpretação do resultado de uma medição de um sistema quântico. As operações que devem ser feitas para se obter os resultados que serão descritos podem ser encontradas em [2], seção 2.2.3.

Dado um operador linear g, se existir um vetor não nulo $|\varphi_\gamma\rangle$ tal que valha a relação

$$g\,|\varphi_\gamma\rangle = \gamma\,|\varphi_\gamma\rangle,$$

chamada usualmente de *equação de autovalores*, então γ é um **autovalor** de g e $|\varphi_\gamma\rangle$ é um **autovetor** associado a esse autovalor. O conjunto de todos os autovalores de um operador linear é chamado de **espectro**.

Existe uma energia mecânica associada a todo sistema mecânico num dado instante de tempo. Em sistemas quânticos isso não é diferente. Assim, a medição de um sistema quântico é uma operação que fornece a energia associada ao sistema num dado instante de tempo.

Conforme será visto na seção 3.2, faz parte da modelagem do estado do sistema quântico um operador hermitiano H, que ajuda a descrever a evolução no tempo do estado do sistema quântico. O espectro de H deve ser interpretado como o conjunto de valores possíveis que a energia pode assumir em estados estacionários (estados puros; no caso da computação quântica, bits). Já os autovetores associados são interpretados como os estados estacionários do sistema [2], pág. 61.

Combinações lineares de vetores que representam estados estacionários também caracterizam estados do sistema quântico, mas estes estados não são estacionários (no caso da computação quântica, qubits). Considere a seguinte combinação linear de estados estacionários

$$|\varphi\rangle = \sum_n c_n |\Phi_n\rangle.$$

O resultado da medição do sistema quando ele se encontra no estado $|\varphi\rangle$ é interpretado da seguinte maneira:

- O resultado de uma medição da energia do sistema quântico é sempre um dos autovalores de H;
- A *probabilidade* de obter um particular resultado E_n é $|c_n|^2$ quando o estado do sistema é descrito pelo vetor $|\varphi\rangle$.

Assim, a energia média do sistema, quando este está no estado $|\varphi\rangle$, será a média ponderada das energias dos estados estacionários incluídos na combinação linear que caracteriza esse vetor, com pesos dados por $|c_n|^2$.

Essa interpretação foi formulada pela primeira vez num postulado escrito por Max Born em 1926 e pode ser vista em mais detalhes em [2], pág 62.

Segue da interpretação probabilística de Born que, ao realizar uma medição num sistema que se encontra no estado $|\varphi\rangle$, obtemos como resposta uma probabilidade $|c_n|^2$ de o sistema estar no estado $|\Phi_n\rangle$ (no qual a energia tem o valor bem definido E_n). Essa é a interpretação utilizada na computação quântica.

A interpretação dada acima sobre a energia de um sistema quântico num dado estado não apresenta problemas no caso de espaços vetoriais de dimensão finita, mas no caso de espaços

de dimensão infinita, as definições dadas até o momento não são suficientes para garantir a existência de uma base de autovetores associada a um operador linear H do sistema. Isso levou Paul Dirac a definir, no seu artigo *The Principles of Quantum Mechanics*, uma classe especial de operadores hermitianos de espaços de dimensão infinita que permitem a análise de vetores de estados quaisquer (estacionários ou não) nos mesmos moldes descritos anteriormente que se aplicam a espaços de dimensão finita. Ele chamou essa classe especial de **observáveis**.

3.2 Evolução temporal do sistema quântico

A descrição da evolução no tempo das propriedades observáveis de um sistema quântico que será considerada neste estudo é a de Schrödinger, que trata os observáveis como operadores independentes do tempo e os vetores de estado da equação diferencial que modela o sistema quântico como os vetores responsáveis pela evolução temporal do sistema, ou seja, como os vetores dependentes do tempo ou vetores dinâmicos. Entretanto, existe ainda a descrição de Heisenberg, que considera os observáveis dependentes do tempo, e exitem também formulações "intermediárias", em que o papel dos agentes dinâmicos é de certa forma repartido entre os observáveis e os vetores de estados.

A equação de Schrödinger, dada de uma maneira simplificada, que mostra a evolução de um estado num sistema quântico é

$$\frac{d\,|\varphi(t)\rangle}{dt} = i\,H\,|\varphi(t)\rangle,$$

onde $|\varphi(t)\rangle$ é um estado do sistema no instante t e H é um operador hermitiano.

Se considerarmos a condição inicial $|\varphi(0)\rangle = v$, onde v é um estado conhecido do sistema, então a solução da equação diferencial acima é

$$|\varphi(t)\rangle = e^{i\,t\,H} v.$$

3.3 A redução do pacote de ondas

Já foi visto o que são medições e como interpretar seus resultados, mas ainda não foi explicado de que forma essas medições são feitas e como descrever o estado do sistema quântico depois de uma medição.

As medições são operações que devem ser realizadas por dispositivos de medida, portanto, é preciso conhecer os efeitos da interação entre o sistema quântico observado e o dispositivo de medida, que pode alterar o estado do sistema submetido ao processo de medição. Por motivos de consistência, é necessário tratar a dinâmica do dispositivo de medida em termos da teoria quântica, assim como o sistema quântico observado.

O conjunto formado pelo sistema submetido à medição mais o dispositivo de medida pode ser visto como um sistema maior, composto por dois subsistemas. Se $\{|\phi_n\rangle\}$ é a base do sistema a ser medido, formada pelos autovetores do observável g que se pretende medir, e se $\{|\Phi_n\rangle\}$ é uma base para o dispositivo de medida, uma base do espaço-produto que corresponde ao espaço vetorial do sistema composto é

$$\{|\phi_r\rangle \otimes |\Phi_s\rangle\} \equiv \{|\phi_r \Phi_s\rangle\},$$

onde $\otimes$ é a notação para produto tensorial[1].

Assim, num estágio inicial o sistema composto se encontra em um estado que pode ser escrito como

$$|\varphi\rangle \otimes |\Phi_0\rangle \equiv \sum_n c_n |\phi_n \Phi_o\rangle,$$

o que significa que o sistema a ser medido e o dispositivo de medida inicializado têm como vetores de estado $|\varphi\rangle \equiv \sum_n c_n |\phi_n\rangle$ e $|\Phi_0\rangle$, respectivamente.

Para que o dispositivo de medida funcione como tal, é suficiente que a dinâmica da interação entre os dois subsistemas de que é formado o sistema composto faça com que ele evolua para um estado final do tipo

$$\sum_n c_n |\chi_n\rangle \otimes |\Phi_n\rangle,$$

em que os coeficientes c_n são os mesmos que aparecem na expansão do estado inicial a ser medido e os estados $|\chi_n\rangle$ são estados quaisquer do sistema que está sendo medido. Este processo é uma *hipótese dinâmica* que presume efeitos da evolução temporal do sistema composto, cuja consistência com a dinâmica quântica foi demonstrada por von Neumann.

Observa-se que os estados finais do sistema de medida são imunes ao princípio de superposição, de forma que combinações lineares destes estados não são estados possíveis do sistema [2]. Com isso percebe-se que o processo de medição interfere no sistema quântico (composto pelo sistema medido e pelo sistema de medida). A equação de Schrödinger que modela a evolução no tempo do estado do sistema não explica porque isso ocorre.

Para tratar essas questões foi introduzido um postulado que preescreve o estado do sistema quântico após a conclusão do processo de medida. Assim, se o sistema que se encontra num estado descrito pelo vetor $|\varphi\rangle$ é submetido a uma mediação do observável g, cujos autovetores são $\{|\phi_n\rangle\}$ associados aos autovalores γ_n, o efeito do processo de medição sobre o estado do sistema medido, após a obtenção do resultado (um particular autovalor γ_n) será $|\phi_n\rangle$, ou seja, o estado é reduzido ao estado estacionário caracterizado pelo autovetor associado ao autovalor obtido na medição. Este postulado é designado como **redução do**

[1] O produto tensorial representa a relação entre o elemento do sistema quântico e os elementos dos subsistemas que o compõem. Assim, se $|\varphi\rangle$ é um elemento de H_1 e $|\psi\rangle$ de H_2, então $|\varphi\rangle \otimes |\psi\rangle$ é um elemento de H, onde H é o sistema composto por H_1 e H_2.

pacote de ondas.

O processo sofrido pelo sistema medido através da interação com o dispositivo de medida é chamado *decoerência*. Ainda é necessário para a teoria quântica um domínio mais concreto dos resultados de medições realizadas e das medições realizáveis [2].

Este capítulo apresentou de uma forma bastante reduzida os principais pontos do formalismo matemático da mecânica quântica de acordo com o capítulo 2, seções 2.1, 2.2, 2.3 e 2.4 do livro [2].

Capítulo 4

Algoritmos quânticos

Embora computadores quânticos com poder de cálculo ainda não sejam conhecidos, devido a dificuldades para transpor alguns problemas como a imprecisão de medições e a decoerência, muitos algoritmos quânticos já foram desenvolvidos, dentre eles os conhecidos algoritmos de Peter Shor [3] para encontrar logaritmos discretos e fatorar inteiros.

A seguir, são apresentados alguns algoritmos quânticos interessantes e úteis.

4.1 Transformada de Fourier Quântica

Como a computação quântica opera com transformações unitárias, é fundamental descrever os processos para construção de algumas destas transformações mais importantes. Uma delas é a transformada de Fourier discreta, que pode ser construída em um computador quântico com complexidade de ordem polinomial, ou seja, existe um polinômio que limita superiormente a função que devolve o número de passos do algoritmo dado o tamanho da entrada, para toda entrada suficientemente grande.

O método para a construção da transformada de Fourier é determinístico, de forma que um computador quântico apenas realiza operações unitárias determinísticas sobre os qubits.

Essa transformada será dada por uma matriz, que chamaremos de A_q, onde as colunas e as linhas representam bits, sendo as colunas bits de entrada e as linhas, de saída.

A transformação é dada da seguinte maneira: considere um número inteiro a, com $0 \leq a < q$, para algum q. A transformação será construída de maneira a levar o estado $|a\rangle$, que é a representação binária de a, para o estado

$$\frac{1}{q^{1/2}} \sum_{c=0}^{q-1} |c\rangle exp\left(\frac{2\pi iac}{q}\right).$$

Será dada uma construção simplificada de A_q para o caso em que q é uma potência de 2, descoberta por Coppersmith (1994) e por Deustsch (1995), independentemente. Portanto, considere $q = 2^l$ e considere a cadeia de caractere $|a\rangle$ escrita da seguinte maneira $|a_{l-1}a_{l-2}...a_0\rangle$. Para a transformação A_q são necessárias duas matrizes unitárias:

- R_j, que opera no $j-$ésimo bit da cadeia:

$$R_j = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \end{array};$$

- e $S_{j,k}$, que opera nos bits da cadeia que estão nas posições j e k, com $j < k$:

$$S_{j,k} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{k-j}} \end{pmatrix} \end{array}.$$

Para executar a transformada de Fourier quântica, aplica-se as matrizes na ordem (da esquerda para direita)

$$R_{l-1}S_{l-2,l-1}R_{l-2}S_{l-3,l-1}S_{l-3,l-2}R_{l-3}...R_1S_{0,l-1}S_{0,l-2}...S_{0,1}R_0.$$

Portanto, para obter a transformada de Fourier A_q quando $q = 2^l$ é necessário aplicar $\frac{l(l-1)}{2}$ matrizes unitárias. Portanto, este algoritmo é consideravelmente mais rápido que a Transformada de Fourier clássica, que é $O(n^2)$.

A aplicação da sequência de transformações acima levará ao estado quântico

$$\frac{1}{q^{1/2}} \sum_b exp\left(\frac{2\pi iac}{q}\right)|b\rangle,$$

onde $|b\rangle$ é a cadeia $|c\rangle$ invertida, ou seja, é a cadeia de bits que se obtém quando se lê a cadeia $|c\rangle$ da direita para a esquerda. Assim, para obter de fato a transformada de Fourier é necessário um algoritmo para inverter a cadeia de bits $|b\rangle$ ou manter os bits na posição em que estão, mas lê-los na ordem inversa. As duas alternativas são de fácil implementação.

Exemplo: Considere a seguinte cadeia de três bits $|a\rangle = |110\rangle$, que em decimal é igual $a = 1*2^2+1*2^1+0*2^0 = 6$. Neste caso $a_0 = 0$, $a_1 = 1$ e $a_2 = 1$ e $l = 3$, logo, $q = 2^3 = 8$. As matrizes acima devem ser aplicadas na ordem $R_2S_{1,2}R_1S_{0,2}S_{0,1}R_0$. Isso irá gerar a seguinte sequência de aplicações:

- $R_2|a_2\rangle = R_2|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad \Longrightarrow \quad |a\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)|10\rangle;$
- $S_{1,2}|a_1a_2\rangle = S_{1,2}|1\rangle\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = S_{1,2}\left(\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \left(\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|11\rangle\right)$
  $= |1\rangle\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right) \quad \Longrightarrow \quad |a\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right)|10\rangle;$
- $R_1|a_1\rangle = R_1|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad \Longrightarrow \quad |a\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle;$

- $S_{0,2}|a_0a_2\rangle = S_{0,2}|0\rangle\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right) = |0\rangle\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right) \implies$
  $\implies |a\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle;$
- $S_{0,1}|a_0a_1\rangle = S_{0,1}|0\rangle\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = |0\rangle\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \implies$
  $\implies |a\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle;$
- $R_0|a_0\rangle = R_0|0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \implies$
  $\implies |a\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}e^{i\pi/2}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right).$

Portanto, expandindo o $|a\rangle$ encontrado, temos que:

$$|a\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + \frac{1}{2\sqrt{2}}|010\rangle - \frac{1}{2\sqrt{2}}|011\rangle - \frac{1}{2\sqrt{2}}e^{i\pi/2}|100\rangle -$$

$$-\frac{1}{2\sqrt{2}}e^{i\pi/2}|101\rangle + \frac{1}{2\sqrt{2}}e^{i\pi/2}|110\rangle + \frac{1}{2\sqrt{2}}e^{i\pi/2}|111\rangle.$$

Logo, obtemos, da sequência de aplicações acima, o seguinte resultado:

$$\frac{1}{2\sqrt{2}}\sum_{b=0}^{7} exp\left(\frac{2\pi i 6c}{8}\right)|b\rangle.$$

Conforme mencionado anteriormente, a Transformada de Fourier é encontrada de fato invertendo-se a cadeia de bits $|b\rangle$, ou seja, fazendo as seguintes substituições:

b	c
$\|000\rangle = 0$	$\|000\rangle = 0$
$\|001\rangle = 1$	$\|100\rangle = 4$
$\|010\rangle = 2$	$\|010\rangle = 2$
$\|011\rangle = 3$	$\|110\rangle = 6$
$\|100\rangle = 4$	$\|001\rangle = 1$
$\|101\rangle = 5$	$\|101\rangle = 5$
$\|110\rangle = 6$	$\|011\rangle = 3$
$\|111\rangle = 7$	$\|111\rangle = 7$

Uma demonstração de que este algoritmo leva de fato a uma Transformada de Fourier pode ser encontrada em [3].

4.2 Fatoração de inteiros

Sabe-se, pelo Teorema Fundamental da Aritmética, que todo inteiro n tem uma decomposição única em primos. Encontrar essa decomposição é um problema que não possui um

algoritmo eficiente. O algoritmo mais rápido conhecido para fatoração de inteiros leva um tempo da ordem de $exp(c(logn)^{1/3}(loglogn)^{2/3})$, para alguma constante c, para realizar a fatoração [3].

Peter Shor, no seu artigo *Algorithms for quantum computation, discrete logarithms and factorizing*, apresentou um algoritmo de complexidade $O((logn)^2(loglogn)(logloglogn))$, acrescido de um pós-processamento de ordem polinomial num computador clássico (já que para este procedimento o computador clássico é mais eficiente) para converter a saída do computador quântico em fatores de n.

Em 1976, Gary L. Miller mostrou que, usando randomização, a fatoração de um inteiro n pode ser reduzida a achar a ordem de um elemento x em um grupo multiplicativo[1] $(mod\, n)$ (mais formalmente $\mathbb{Z}_n$), ou seja, encontrar o menor r tal que $x^r \equiv 1\,(mod\, n)$. Assim, Shor propôs um algoritmo para este problema.

Para achar o fator de um número ímpar n (se n for par, deve-se dividí-lo por 2, seu fator primo trivial, até chegar em um número ímpar), dado um método para calcular a ordem r de x, é preciso:

1. escolher um número aleatório $x\,(mod\, n)$;
2. encontrar sua ordem r (com o método existente);
3. calcular $mdc\,(x^{r/2} - 1, n)$, que irá resultar num fator de n.

No passo 3 pode ser usado o algoritmo de Euclides, que é de ordem polinomial. Como $x^r \equiv 1\,(mod\, n)$, temos que

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

Assim, o cálculo do $mdc\,(x^{r/2} - 1, n)$ só vai falhar em achar um divisor não-trivial de n se r for ímpar (assim $x^{r/2}$ não será inteiro) ou se $x^{r/2} \equiv -1(mod\, n)$. Este procedimento irá gerar um fator de n com probabilidade de no mínimo $1 - 1/2^{k-1}$, onde k é o número de fatores primos ímpares distintos de n. A demonstração deste resultado pode ser encontrada em [3].

Enquanto n for ímpar e não for uma potência de um primo (existem algoritmos clássicos eficientes para este problema em particular), este esquema poderá ser repetido e irá funcionar dentro dos limites estabelecidos.

Basta agora descrever o algoritmo que deve ser usado no passo 2 e implementado em um computador quântico.

Dados x e n, para achar a ordem de x, isto é, o menor r tal que $x^r \equiv 1\,(mod\, n)$ é necessário, primeiramente, encontrar q, uma potência de 2 de modo que $n^2 \leq q < 2n^2$. Em

[1] Grupo é um conjunto fechado para uma operação binária, neste caso a multiplicação, que deve satisfazer as propriedades associativa, existência de identidade e inverso [12].

seguida, coloca-se o primeiro registro, que irá representar os números $a\,(mod\,q)$, no seguinte estado, conhecido como estado uniforme de superposições,

$$\frac{1}{q^{1/2}}\sum_{a=0}^{q-1}|a\rangle|0\rangle.$$

Em seguida, calcula-se $x^a\,(mod\,n)$ no segundo registro da seguinte forma:

```
power := 1
for i := 0 to l − 1 do
  if (a_i == 1) then
    power := power ∗ x^(2^i) (mod n)
  end if
end for
```

Logo, o sistema fica no seguinte estado:

$$\frac{1}{q^{1/2}}\sum_{a=0}^{q-1}|a\rangle|x^a(mod\,n)\rangle.$$

Em seguida, aplica-se a Transformada de Fourier, como definida na seção anterior, no primeiro registro, o que vai fazer com que o estado $|a\rangle$ seja levado ao estado

$$\frac{1}{q^{1/2}}\sum_{c=0}^{q-1}exp\left(\frac{2\pi iac}{q}\right)|c\rangle.$$

Assim, o sistema ficará no estado

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}exp\left(\frac{2\pi iac}{q}\right)|c\rangle|x^a(mod\,n)\rangle.$$

Finalmente faz-se uma medição no sistema. Assim, obtém-se uma probabilidade do sistema estar num determinado estado $|c, x^k(mod\,n)\rangle$, que é obtida somando-se todas as maneiras possíveis de se atingir este estado. A probabilidade encontrada é

$$\left|\frac{1}{q}\sum_{a:x^a\equiv x^k}exp\left(\frac{2\pi iac}{q}\right)\right|^2,$$

onde a soma é feita sobre a, com $0 \leq a < q$, tal que $x^a \equiv x^k(mod\,n)$.

Essa probabilidade será de no mínimo $1/3r^2$ para n suficientemente grande [3]. Portanto, depois de obtido o valor da probabilidade, é possível encontrar o valor de r, que era o objetivo deste passo do algoritmo.

São necessárias algumas suposições e aproximações para chegar no resultado mencionado. Devido ao fato de que aproximações são feitas para que o cálculo de r possa ser efetuado, é necessário demonstrar que o erro cometido nas aproximações é de ordem pequena. Todas estas demonstrações necessárias para provar que a probabilidade de se encontrar r com o

algoritmo proposto é alta podem ser encontradas em [3].

Nolan R. Wallach, em seu artigo *Quantum computing and entanglement for mathematicians*, propôs uma interpretação diferente para o problema da fatoração. Ao invés de encarar a redução do problema da fatoração como o problema de encontrar a ordem de um elemento x em um grupo multiplicativo $(mod\, n)$, que foi o caminho seguido por Shor, ele interpretou a redução como o problema de encontrar o menor período de uma função f, definida em $\mathbb{N} \to \mathbb{Z}_{\mathbb{N}}$. O algoritmo para este problema segue os mesmos passos do algoritmo desenvolvido por Shor e pode ser visto em [1].

Note que este algoritmo, como todos os algoritmos quânticos conhecidos, é um algoritmo probabilístico, pois está associado a uma probabilidade que é dada quando se realiza uma medição. Desta forma, é fácil concluir que todo algoritmo quântico deve levar em conta a necessidade de aumentar o coeficiente associado a saída desejada, de maneira que quando uma medição for feita, a probabilidade de ter a saída desejada seja alta.

4.3 Busca desordenada

Para fazer uma busca de uma informação específica em meio a muitos dados desordenados, o algoritmo clássico leva um tempo da ordem de O(N), onde N é a quantidade de dados que se tem. Em 1997, Lov K. Grover criou um algoritmo quântico que realiza essa busca levando um tempo de ordem $\mathrm{O}(\sqrt{N})$.

O algoritmo de busca consiste em fazer uma sequência de operações unitárias, seguidas de uma medição. Para as operações unitárias serão usadas três matrizes, duas delas muito utilizadas em algoritmos quânticos e bastante parecidas com as matrizes R_j e $S_{j,k}$ utilizadas no algoritmo da Tranformada de Fourier quântica. As matrizes são as seguintes:

- Transformação de Walsh-Hadamard:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

- Matriz de rotação:

$$R = \begin{bmatrix} e^{\phi_1 i} & 0 \\ 0 & e^{\phi_2 i} \end{bmatrix},$$

  onde ϕ_1 e ϕ_2 são números reais arbitrários.

- Matriz de Difusão:

$$D = \begin{bmatrix} -1+\frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & -1+\frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & -1+\frac{2}{N} \end{bmatrix}_{n \times n}.$$

O problema é formalizado da seguinte maneira: considere um sistema com $N = 2^n$ estados chamados $S_1, S_2, ..., S_N$. Esses 2^n estados são representados por cadeias de bits de tamanho n. Suponha que exista um único estado S_v tal que $C(S_v) = 1$, enquanto que para todos os outros estados S, $C(S) = 0$. O problema é encontrar o estado S_v.

O algoritmo para a solução deste problema segue os seguintes passos:

1. Inicializar o sistema no estado $\frac{1}{\sqrt{N}} \sum_N |S_N\rangle$, ou seja, atribuir o mesmo coeficiente para todos os estados do sistema;

2. Repetir as seguintes operações unitárias $\mathrm{O}(\sqrt{N})$ vezes (será explicado a seguir o motivo deste número de repetições):

   - Seja S o estado em que o sistema está. Se $C(S) = 1$, aplicar a matriz R de forma a rotacionar a fase em π radianos. Se $C(S) = 0$, não alterar o sitema;
   - Aplicar a matriz de difusão D;

3. Medir o sistema. O resultado será o estado S_v procurado com probabilidade de mínimo 0.7.

O ponto mais importante do algoritmo está no passo 2. Cada iteração feita neste *loop* aumenta o valor do coeficiente do estado S_v desejado em $\mathrm{O}\left(\frac{1}{\sqrt{N}}\right)$. Assim, ao final de $\mathrm{O}(\sqrt{N})$ repetições do *loop* o valor do coeficiente do estado desejado passa a ser $\mathrm{O}(1)$.

Para ver que o valor do coeficiente do estado desejado aumenta em $\mathrm{O}\left(\frac{1}{\sqrt{N}}\right)$ a cada iteração, é necessário ver, em primeiro lugar, que a aplicação da matriz de difusão D pode ser interpretada como uma operação de *inversão em relação a média.*

Seja α a média dos coeficientes de todos os estados do sistema, ou seja

$$\alpha = \frac{1}{N} \sum_{i=1}^{N} \alpha_i.$$

Como resultado da aplicação da matriz D, a magnitude do coeficiente de cada estado aumenta (diminui) de forma que, depois da aplicação, o valor do coeficiente estará abaixo (acima) da média o mesmo tanto que estava acima (abaixo) antes da aplicação, como pode ser visto na Figura 4.1.

Observe que a matriz D pode ser decomposta na forma $D = -I + 2P$, onde I é a matriz identidade e P é um operador de projeção, conforme visto na Seção 3.1.2. Note que, quando aplica-se P a um vetor v, obtemos o seguinte resultado

$$\begin{bmatrix} \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ \vdots & \vdots & & \vdots \\ \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{bmatrix} = \begin{bmatrix} \frac{1}{N}(v_1 + v_2 + \ldots + v_N) \\ \frac{1}{N}(v_1 + v_2 + \ldots + v_N) \\ \vdots \\ \frac{1}{N}(v_1 + v_2 + \ldots + v_N) \end{bmatrix}. \tag{4.1}$$

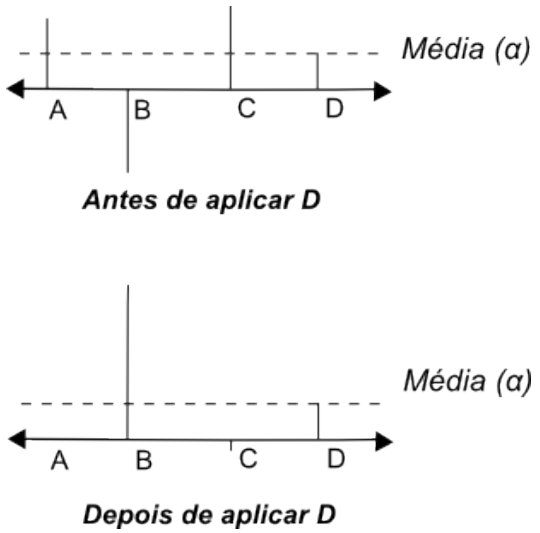

Figura 4.1: Inversão em relação a média

Observe que o vetor resultante é tal que cada componente é igual a média de todas as componentes.

Para ver que D é de fato uma inversão em relação a média, note que quando aplica-se D a um vetor v, temos que

$$Dv = (-I + 2P)v = -v + 2Pv. \tag{4.2}$$

Do resultado obtido em (4.1), segue que cada componente do vetor Pv é a média de todas as componentes. Seja A essa média. Note,então, que a i-ésima componente do vetor Dv é $(-v_i + 2A)$, que pode ser escrita como $(A + (A - v_i))$, que é exatamente a inversão em relação a média.

Finalmente, para terminar de mostrar que a cada iteração do passo 2 do algoritmo o valor do coeficiente do estado desejado S_v aumenta em $\mathrm{O}\left(\frac{1}{\sqrt{N}}\right)$, considere um vetor onde cada componente, exceto uma, tem um coeficiente igual a $C/\sqrt{N}$, com $1/2 < C < 1$, e a componente diferente tem um coeficiente cujo valor é $-\sqrt{1 - C^2}$. A média de todas as componentes é aproximadamente igual a $C/\sqrt{N}$. Como $N - 1$ componentes desse vetor são aproximadamente iguais a média, a aplicação de D sobre esse vetor não vai causar mudanças significativas nessas componentes. Já a componente diferente das demais, cujo valor era negativo, se torna positivo e seu valor aumenta em $2C/\sqrt{N}$, como pode ser visto na Figura 4.2.

Assim, no *loop* do passo 2, inicialmente o valor do coeficiente de um estado selecionado é invertido (pela matriz de rotação). Em seguida aplica-se a operação de inversão em relação a média. Isso aumenta o valor do coeficiente do estado selecionado em $2C/\sqrt{N}$. Portanto, se a magnitude do coeficiente do estado selecionado, isto é $\sqrt{1 - C^2}$, for menor que $1/\sqrt{2}$, o aumento no seu valor a cada iteração é maior que $1/\sqrt{2N}$. Ou seja, se

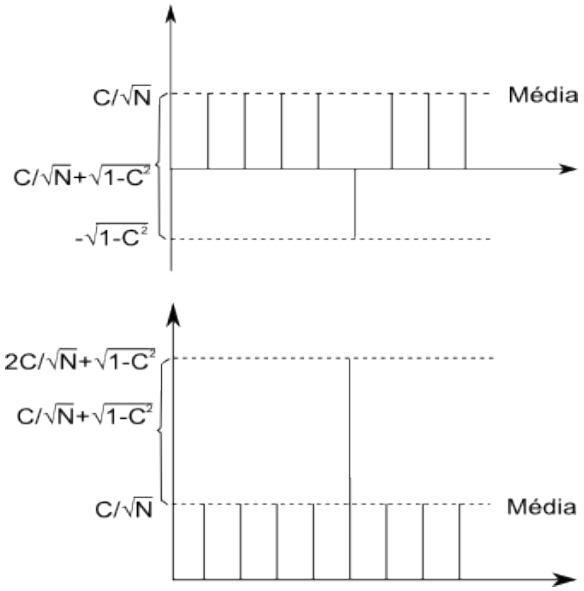

Figura 4.2: O valor da componente diferente da média aumenta em $2C/\sqrt{N}$, enquanto as demais permanecem praticamente inalteradas

$$\sqrt{1-C^2} < \frac{1}{\sqrt{2}} \Longrightarrow \sqrt{1-C^2} + \frac{2C}{\sqrt{N}} < \frac{1}{\sqrt{2}} + \frac{2C}{\sqrt{N}} = \frac{\sqrt{N}+2\sqrt{2}C}{\sqrt{2N}}, \tag{4.3}$$

como

$$\frac{\sqrt{N}+2\sqrt{2}C}{\sqrt{2N}} \simeq \frac{\sqrt{N}+2.83C}{\sqrt{2N}} > \frac{1}{\sqrt{2N}}, \qquad \text{para qualquer } C, \tag{4.4}$$

então segue que, de fato, o aumento do valor do coeficiente é maior que $1/\sqrt{2N}$.

Isso implica que, $\exists M < \sqrt{N}$ tal que depois de M repetições do *loop* do passo 2, a magnitude do valor do coeficiente do estado desejado será maior que $1/\sqrt{2}$, isto é,

$$\frac{M}{\sqrt{2N}} > \frac{M}{\sqrt{2}M} = \frac{1}{\sqrt{2}} \simeq 0.71. \tag{4.5}$$

Portanto, se o sistema for medido agora, ele estará no estado desejado com uma probabilidade maior do que 0.7.

Note que este algoritmo também é probabilístico.

Capítulo 5

Correção de erros

Conforme dito anteriormente, uma das dificuldades na construção de um computador quântico é a decoerência, que é o processo sofrido pelo sistema quântico medido devido a interação com o dispositivo de medida. Assim, quando há a necessidade de se realizar muitas medições durante a execução de um algoritmo, os estragos sofridos pelo sistema medido são enormes, de forma que muita informação é perdida, comprometendo os resultados da execução [2].

Porém, existem maneiras de se diminuir a taxa de decoerência de sistemas quânticos, por meio de codificações que diminuem a perda de dados no sistema. Esse é o análogo quântico do problema clássico de transmitir uma informação através de um canal que pode sofrer interferências, chamadas ruídos. Neste caso, os códigos para correção de erros podem ser aplicados para recuperar com uma alta probabilidade a informação transmitida, mesmo que uma parte desta informação tenha sido corrompida durante a transmissão.

Para o estudo dessas codificações, algumas suposições são necessárias para tornar o problema mais simples e a resolução mais factível:

- Assume-se que a decoerência ocorre de maneira independente em cada qubit;
- Considera-se que apenas um bit de cada qubit é afetado por vez (essa hipótese é equivalente às hipóteses do análogo clássico de transmitir um sinal através de um canal que sofre interferências e é razoável em muitas situações [6]);
- Assume-se que não ocorrem erros durante as operações (essa aproximação é razoável considerando-se que o tempo para realizar operações é pequeno o suficiente para que um estado do sistema não sofra mudanças significativas nesse período [1]; além disso, os erros que podem ocorrer nas operações são pequenos quando comparados aos erros causados pela decoerência e corrigidos pelas codificações [6]).

O objetivo das codificações é preservar um espaço vetorial de dimensão k de erros. Para isso, mapeamos os estados deste espaço para um espaço vetorial de Hilbert de dimensão n maior do que k.

Segue a nomenclatura usada para descrever o problema:

- Código quântico (n, k): subespaço de dimensão k de um espaço de Hilbert de dimensão n;
- $\mathcal{H}$: espaço de Hilbert de dimensão n, do tópico anterior, chamado de espaço codificado;
- $\mathcal{Q}$: espaço de Hilbert de dimensão k;
- $\mathcal{C}$: código;
- E: operador de codificação para $\mathcal{C}$, que age de $\mathcal{Q}$ para $\mathcal{C}$;

Será considerado o caso em que $k = 2^d$ e $n = 2^r$, com $d < r$.

Com o próposito de simplificar o problema da codificação é introduzida a ideia de operadores de recuperação, pois o uso destes operadores permite que se ignorem detalhes de implementação que não são relevantes para as propriedades da correção de erros.

Um operador de recuperação $\mathcal{R}$ é um operador do espaço codificado $\mathcal{H}$ que é usado para restaurar um estado depois que ele foi afetado pela decoerência. Na prática, estes operadores são implementados como uma combinação de operadores unitários e medições.

Um código quântico para correção de erro é, então, um par $(\mathcal{C}, \mathcal{R})$, que consiste de um código quântico e um operador de recuperação. As propriedades desse código quântico dependem da interação do sistema quântico (cujos estados serão codificados para correção de erros) com o dispositivo de medida ou com o ambiente em que o sistema se encontra.

Considera-se que os efeitos sofridos por um estado quântico, devido a sua interação com o ambiente, podem ser descritos por operadores lineares de $\mathcal{Q}$. A família desses operadores será chamada de $\mathcal{A}$, com $\mathcal{A} = \{A_0, ...\}$.

Da mesma forma que no análogo clássico, em geral, é impossível corrigir $\mathcal{A}$ de forma a reduzir o erro a 0. Portanto, é importante corrigir os principais membros de $\mathcal{A}$. Isso leva ao estudo de códicos quânticos para correção de e erros.

Um operador A agindo sobre $\mathcal{H}$ induz no máximo e erros se ele for um produto tensorial de r operadores onde $r - e$ deles são a identidade. Assim, um código para correção de e erros pode recuperar a informação de qubits que foram afetados pela sua interação com uma família de operadores lineares $\mathcal{A}$ que induzem no máximo e erros.

Para desenvolver esses códigos para correção de erros é necessário ter uma base para a família $\mathcal{A}$ de operadores lineares. Uma das bases que pode ser considerada para o caso em que os operadores interagem com qubits de tamanho 1 (que ainda tem a propriedade de que cada um de seus operadores é unitário) é a seguinte:

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \quad A_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \quad A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad A_3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{5.1}$$

Esses operadores, fisicamente, correspondem a: 0) deixar o sistema inalterado, 1) mudar o sinal do bit se ele estiver no estado $|1\rangle$, 2) trocar o bit (se ele estiver em $|0\rangle$, mudar para

$|1\rangle$, e vice-versa), 3) trocar o bit e mudar o sinal se ele estivesse em $|1\rangle$. Esses são todos os erros que podem ser causados a um qubit.

Outra base útil que pode ser considerada é a seguinte:

$$\tilde{A}_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}; \quad \tilde{A}_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}; \quad \tilde{A}_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}; \quad \tilde{A}_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}. \tag{5.2}$$

Os operadores $\tilde{A}_0$ e $\tilde{A}_1$ implementam uma medição ideal de um bit. Os operadores $\tilde{A}_2$ e $\tilde{A}_3$ implementam uma medição ideal seguida de uma troca de bits.

É necessário determinar o tamanho mínimo que o espaço de Hilbert $\mathcal{H}$ deve ter para acomodar os qubits codificados. Considerando que apenas um qubit sofre decoerência por vez (conforme as suposições iniciais para simplificar o problema), tem-se que a família $\mathcal{A}$ induz no máximo um erro. Note que os erros que um bit pode sofrer são três (ter seu valor trocado, ter seu sinal trocado, ter seu valor e seu sinal trocado), conforme mencionado em (5.1). Portanto, é preciso mapear os qubits para um espaço de Hilbert cuja dimensão seja grande o suficiente para acomodar todas as possibilidades resultantes da ação de cada um dos três erros sobre cada um dos bits de um qubit e mais a possibilidade de não ocorrerem erros. Assim, dada uma cadeia de n bits, a ação de todos os erros sobre cada bit e mais a possibilidade de não ocorrerem erros resulta num total de $3n + 1$. É necessário dobrar esse valor para acomodar os dois estados ($|0\rangle$ e $|1\rangle$) e todas as suas possibilidades de erro. Assim, chegamos ao valor $2(3n + 1)$. Logo, lembrando que estamos considerando o caso em que o tamanho do espaço de Hilbert é uma potência de 2, chega-se a conclusão que a dimensão do espaço deve ser tal que $2(3n + 1) \leq 2^n$, ou seja, $n \geq 5$.

Peter Shor propôs uma codificação em que $n = 9$, em 1995 [4]. Já em 1996, Laflamme propôs uma codificação em que $n = 5$ [7], que é o valor mínimo. Será descrita a codificação estabelecida por Peter Shor, por ser mais natural e por não fixar valores descobertos heuristicamente, como é o caso de Laflamme.

Cada qubit deve ser codificado por um operador de codificação E da seguinte maneira:

$$|0\rangle \longrightarrow \frac{1}{2\sqrt{2}} \left(|000\rangle + |111\rangle\right) \left(|000\rangle + |111\rangle\right) \left(|000\rangle + |111\rangle\right),$$

$$|1\rangle \longrightarrow \frac{1}{2\sqrt{2}} \left(|000\rangle - |111\rangle\right) \left(|000\rangle - |111\rangle\right) \left(|000\rangle - |111\rangle\right).$$

Note que esse procedimento irá gerar, para cada bit da cadeia, um qubit de tamanho 9.

Considere agora que uma medição é feita após essa codificação. Se não ocorreu decoerência, os três grupos que formam o bit $|0\rangle$ codificado estarão em $|000\rangle + |111\rangle$. Da mesma maneira, para o bit $|1\rangle$, as três cadeias de bits estarão em $|000\rangle - |111\rangle$. Se ocorreu decoerência, um dos 9 bits da cadeia mudou e, consequentemente, um dos três grupos estará diferente. Para saber qual era o bit original, basta olhar para os dois grupos que são iguais. Entretanto, isso não é o suficiente para restaurar um qubit ao seu estado original, pois ao

medir-se os qubits codificados novas alterações são causadas neles.

Para preservar de fato os qubits codificados é necessário medir a decoerência sem medir o estado dos qubits. Isso permite reverter a decoerência. Para entender como é possível fazer isso é preciso estudar o processo da decoerência mais detalhadamente.

A decoerência é descrita como uma transformação unitária que causa um emaranhado entre os qubits de sistema quântico e os qubits do dispositivo de medida. É possível descrever este processo mostrando o que acontece com os qubits $|0\rangle$ e $|1\rangle$ quando afetados pela decoerência. Será considerado que o primeiro qubit da cadeia codificada sofre decoerência, mas o processo é análogo para qualquer um dos outros oito qubits.

O processo de decoerência é

$$|e_0\rangle|0\rangle \longrightarrow |a_0\rangle|0\rangle + |a_1\rangle|1\rangle$$

$$|e_0\rangle|1\rangle \longrightarrow |a_2\rangle|0\rangle + |a_3\rangle|1\rangle,$$

onde $|a_0\rangle$, $|a_1\rangle$, $|a_2\rangle$ e $|a_3\rangle$ são estados do dispositivo de medida.

Observe o que acontece com o estado $|0\rangle$ codificado, isto é, com a superposição $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Depois da decoerência, este estado passa para a superposição

$$\frac{1}{\sqrt{2}}\left[(|a_0\rangle|0\rangle + |a_1\rangle|1\rangle)\,|00\rangle + (|a_2\rangle|0\rangle + |a_3\rangle|1\rangle)\,|11\rangle\right].$$

Reescrevendo em termos da base de Bell[1], obtém-se

$$\frac{1}{2\sqrt{2}}\left(|a_0\rangle + |a_3\rangle\right)\left(|000\rangle + |111\rangle\right) + \frac{1}{2\sqrt{2}}\left(|a_0\rangle - |a_3\rangle\right)\left(|000\rangle - |111\rangle\right) +$$

$$+\frac{1}{2\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)\left(|100\rangle + |011\rangle\right) + \frac{1}{2\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)\left(|100\rangle - |011\rangle\right).$$

Similarmente, o qubit codificado $|1\rangle$, ou seja, a superposição $\frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)$ depois da decoerência e escrita na base de Bell vai para o estado

$$\frac{1}{2\sqrt{2}}\left(|a_0\rangle + |a_3\rangle\right)\left(|000\rangle - |111\rangle\right) + \frac{1}{2\sqrt{2}}\left(|a_0\rangle - |a_3\rangle\right)\left(|000\rangle + |111\rangle\right) +$$

$$+\frac{1}{2\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)\left(|100\rangle - |011\rangle\right) + \frac{1}{2\sqrt{2}}\left(|a_1\rangle + |a_2\rangle\right)\left(|100\rangle + |011\rangle\right).$$

Note que os coeficientes do dispositivo de medida, após a decoerência, são os mesmos para os qubits codificados $|0\rangle$ e $|1\rangle$. Então, pode-se restaurar o estado codificado e manter-se a evolução do sistema criando-se alguns qubits auxiliares que indicarão qual qubit sofreu decoerência e se o sinal dos vetores da base de Bell mudou. Assim, medindo estes qubits

[1] A base de Bell é uma base para um espaço de Hilbert onde os vetores da base são definidos em termos de bases computacionais. Os vetores da base de Bell são $|000\rangle \pm |111\rangle$, $|001\rangle \pm |110\rangle$, $|010\rangle \pm |101\rangle$, $|100\rangle \pm |011\rangle$.

auxiliares é possível restaurar o estado original de um qubit.

Essa restauração consiste primeiro em uma transformação unitária realizada por um computador quântico e depois em uma medição de alguns qubits resultantes da transformação. O primeiro passo que o computador deve executar é comparar todos os três grupos que formam o qubit codificado escritos na base de Bell. Se os três grupos são iguais, o resultado que o qubit auxiliar deve indicar é "não houve decoerência", e o qubit deve ser mantido como está. Se os três grupos não são iguais, os qubits auxiliares devem indicar qual grupo está diferente e como ele está. Por exemplo, considere que o qubit auxiliar $|q_1\rangle$ deva indicar se houve ou não decoerência; assim, se não houve decoerência, atribui-se o valor $|0\rangle$ a ele, caso contrário, atribui-se o valor $|1\rangle$. Caso tenha ocorrido decoerência, considere que o qubit auxiliar $|q_2\rangle$ deva indicar se o primeiro grupo de qubits é o grupo diferente; assim, se o grupo em questão não for o grupo diferente, atribui o valor $|0\rangle$ para ele, caso contrário, $|1\rangle$. E assim por diante. Em seguida, baseado nas informaçõs dos qubits auxiliares, o computador deve restaurar os qubits do sistema aos seus estados originais. Portanto, a análise do sistema e a devida atribuição de valores aos qubits auxiliares são realizadas por meio de transformações lineares e a medição dos qubits auxiliares implicarão na correta restauração do sistema. Isso deve ser implementado usando-se operadores de recuperação $\mathcal{R}$, já descritos anteriormente.

Conforme simplificação feita no início do capítulo, este esquema funciona somente no caso em que apenas um bit sofre decoerência. Note que se p é a probabilidade de um bit sofrer decoerência, então a probabilidade de k bits não sofrerem decoerência é $(1-p)^k$. No esquema de codificação dado, cada bit é substituído por 9 bits. Então a probabilidade de pelo menos 2 dos 9 bits que formam um qubit codificado sofrerem decoerência é

$$\sum_{k=2}^{9} \binom{9}{k} p^k (1-p)^{9-k} = \binom{9}{2} p^2 (1-p)^7 + \ ... \ + \binom{9}{9} p^9 = 36p^2(1-p)^7 + \ ... \ +$$

$$+9p^8(1-p) + p^9 = 1 - (1+8p)(1-p)^8 \approx 36p^2.$$

Portanto, se temos um sistema com r qubits, a probabilidade de que ocorra apenas um erro em cada um deles, de forma que os $9r$ qubits do sistema codificado possam ser decodificados para obterem-se os qubits originais é $(1-36p^2)^r$. Assim, se $p < 1/36$, e $r = 10$ por exemplo, a probabilidade de se corrigir erros com este esquema é maior que 80%.

Capítulo 6

Medidas de emaranhados

Neste capítulo iremos mostrar uma aplicação da teoria de Lie na computação quântica. Vamos tratar da estrutura de órbitas encontradas quando aplicamos transformações locais sobre estados puros e mostrar um exemplo de medida de emaranhado, que é uma função que permite determinar se dois estados quânticos estão relacionados por transformações locais. Vamos nos restringir as cadeias de qubits de tamanho 2.

6.1 Emaranhados

Um estado quântico que não pode ser escrito como um produto tensorial de estados puros é chamado de estado emaranhado, como por exemplo o estado

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right).$$

Uma outra maneira de identificar um estado emaranhado é utilizando o conceito de *transformação local*.

Uma transformação quântica local num qubit de tamanho n é dada por um operador unitário da forma

$$A_1 \otimes A_2 \otimes ... \otimes A_n,$$

onde $A_i \in U(2)$, que é o grupo dos operadores unitários de $\mathbb{C}$ quando munido de produto de matrizes.

Não existe uma transformação local que leve o estado $|\varphi\rangle$, acima, ao estado puro $|00\rangle$ (nem ao $|11\rangle$), o que também caracteriza $|\varphi\rangle$ como um estado emaranhado. Outra denominação que se dá neste caso é que o estado $|\varphi\rangle$ *não está na órbita* de $|00\rangle$ (ou de $|11\rangle$) sob transformação local.

O grupo de operadores unitários $U(2)$ e o grupo de operadores lineares especiais que possuem determinante igual a um $SL(2,\mathbb{C})$ (este último aparecerá na próxima seção) são descritos como

$$U(2) = \{x \in GL(2,\mathbb{C}) \mid x\,x^\dagger = 1\}$$
$$SL(2,\mathbb{C}) = \{x \in GL(2,\mathbb{C}) \mid det\,x = 1\},$$

onde $GL(2,\mathbb{C})$ é o grupo de todas as matrizes complexas não singulares. Este conjunto é um exemplo de um grupo de Lie, que são grupos com estrutura topológica que tornam os produtos de elementos do grupo e a inversão funções diferenciáveis. Isso significa que podemos fazer cálculo diferencial e integral com esses objetos.

6.2 Medidas de emaranhados

A aplicação de $G = SL(2,\mathbb{C})$ x $SL(2,\mathbb{C})$ em $V = \mathbb{C}^2 \otimes \mathbb{C}^2$ deixa invariante uma forma bilinear, cuja notação é $(\ ,\ )$, e que é dada nos elementos da base por

$$(|00\rangle, |11\rangle) = (|11\rangle, |00\rangle) = 1$$
$$(|01\rangle, |10\rangle) = (|10\rangle, |01\rangle) = -1$$

e todos os outros produtos são 0.

Vamos analisar o estado $\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}, \frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)$. Note que

$$\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{1}{2}\left(|00\rangle + |11\rangle, |00\rangle + |11\rangle\right) =$$
$$= \frac{1}{2}\left[(|00\rangle, |00\rangle + |11\rangle) + (|11\rangle, |00\rangle + |11\rangle)\right] =$$
$$= \frac{1}{2}\left[(|00\rangle, |00\rangle) + (|00\rangle, |11\rangle) + (|11\rangle, |00\rangle) + (|11\rangle, |11\rangle)\right] =$$
$$\frac{1}{2}(0 + 1 + 1 + 0) = 1.$$

Como $(|00\rangle, |00\rangle) = 0$, não pode existir uma transformação local levando $|00\rangle$ a $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ e vice-versa, já que uma função da forma $\phi(u) = |(u,u)|$ é invariante sob transformações locais. Esta função é um exemplo de medida de emaranhado. De fato, devido à maneira como a forma bilinear está definida, um estado u é um estado emaranhado se e somente se $\phi(u) > 0$.

Esta função tem ainda mais duas propriedades: para todo estado u, $\phi(u) \leq 1$; e $\phi(u) = 1$ se e somente se u está na órbita de $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ sob transformações locais.

Para provar a primeira propriedade, considere que $u = a|00\rangle + b|01\rangle + c|10\rangle + |11\rangle$. Então

$$\phi(u) = |(u,u)| = |a^2(|00\rangle, |00\rangle) + ab(|00\rangle, |01\rangle) + ac(|00\rangle, |10\rangle) + ad(|00\rangle, |11\rangle) +$$
$$+ba(|01\rangle, |00\rangle) + b^2(|01\rangle, |01\rangle) + bc(|01\rangle, |10\rangle) + bd(|01\rangle, |11\rangle) +$$
$$+ca(|10\rangle, |00\rangle) + cb(|10\rangle, |01\rangle) + c^2(|10\rangle, |10\rangle) + cd(|10\rangle, |11\rangle) +$$

$$+da(|11\rangle,|00\rangle)+db(|11\rangle,|01\rangle)+dc(|11\rangle,|10\rangle)+d^2(|11\rangle,|11\rangle)|=2|ad-bc|.$$

Como

$$2|ad-bc|\leq 2|ad|+2|bc| \quad e$$

$$2|ad|=2|a||d|\leq |a|^2+|d|^2 \quad \text{(idem para } 2|bc|),$$

então

$$\phi(u)=2|ad-bc|\leq |a|^2+|b|^2+|c|^2+|d|^2=1,$$

como queríamos demonstrar.

Para provar a afirmação sobre a órbita, isto é, que $\phi(u)=1$ se e somente se u está na órbita de $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, será considerado o seguinte teorema:

Teorema 1 *Considere que G é um produto de n cópias de $SL(2,\mathbb{C})$ e K n cópias de $SU(2)$. Seja G um grupo de Lie semisimples sobre $\mathbb{C}$ e K um subgrupo compacto maximal de G. Seja (π,V) uma representação analítica finita de G, munida do produto hermitiano (de espaços de Hilbert) $\langle\ |\ \rangle$, que é invariante sobre K. Considere ainda $v\in V$ e $u\in\pi(G)v$. Se $m=inf\{\langle\pi(g)v|\pi(g)v\rangle\mid g\in G\}$ e $\langle u|u\rangle=m$ então $\pi(K)u=\{w\in\pi(G)v\mid\langle w|w\rangle=m\}$. Além disso, o ínfimo é atingido se e somente se a órbita $\pi(G)v$ for fechada.*

Este teorema diz que se G é um grupo que age num espaço de Hilbert V, e Gv é a órbita por um elemento v deste espaço, ou seja,

$$Gv=\{gv\mid g\in G\},$$

então, pegando todos os elementos de Gv que tem norma mínima, obtemos um subconjunto que é, de fato, a órbita Ku de algum elemento u de Gv por um subgrupo K de G, que é compacto e maximal. Uma ideia da demonstração pode ser encontrada em [1] e a demonstração completa se encontra no artigo *The length of vectors in representation spaces. Algebraic geometry*, de George Kempf e Linda Ness.

Vamos ver agora como este resultado se aplica à nossa situação. Note que ao agir sobre o espaço $V=\mathbb{C}^2\otimes\mathbb{C}^2$, o grupo $G=SL(2,\mathbb{C})$ x $SL(2,\mathbb{C})$ gera a seguinte estrutura de órbita: para cada $\lambda\in\mathbb{C}-0$, o conjunto

$$M_\lambda=\{v\in V\mid(v,v)=\lambda\}$$

é uma órbita.

Note ainda que como $(|00\rangle,|00\rangle)=0$ e como o grupo G preserva o produto bilinear definido, então $(g|00\rangle,g|00\rangle)=0$ para todo $g\in G$, isto é, $G|00\rangle$ está contido em M_0. Além disso, o elemento $\{0\}$ também está contido em M_0, embora não faça parte da órbita de $|00\rangle$ (pois 0 não pertence a G).

Considere $u_0 = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Já sabemos que $(u_0, u_0) = 1$, então, da propriedade do produto interno, segue que $(zu_0, zu_0) = z^2$, onde $z \in \mathbb{C}$. Como para cada $g \in G$ temos que $g(zu_0) = zg(u_0)$ então a órbita de zu_0, que é Gzu_0, é igual à orbita zGu_0. Portanto, se $z \neq 0$, temos que $G(zu_0) = M_{z^2}$.

Precisamos maximar a função ϕ em S^3 (esfera de raio unitário vista na Seção 2.2), para encontrar w tal que $\phi(w) = 1$, que é seu valor máximo conforme vimos na demonstração da propriedade anterior. Note que qualquer que seja w, ele vai pertencer a algum M_λ. Como $M_\lambda = zGu_0$, temos então que existe algum $z_1 \in \mathbb{C}$ e algum $g \in G$ tal que

$$w = z_1 g u_0. \tag{6.1}$$

Considere z_1 escrito na sua forma polar

$$z_1 = re^{i\theta}. \tag{6.2}$$

Substituindo (6.2) em (6.1) temos que

$$w = re^{i\theta} g u_0. \tag{6.3}$$

Como $w \in S^3$, temos que

$$1 = ||w|| = ||re^{i\theta} g u_0|| = |re^{i\theta}|\,||gu_0|| = r|e^{i\theta}|\,||gu_0|| = r(\sqrt{cos^2 2\theta + sen^2 2\theta})||gu_0|| =$$

$$= r||gu_0|| \quad \Longleftrightarrow \quad r = \frac{1}{||gu_0||}. \tag{6.4}$$

Substituindo (6.4) em (6.3) temos que

$$w = e^{i\theta}\frac{gu_0}{||gu_0||}. \tag{6.5}$$

Para tal w temos que

$$\phi(w) = |(w,w)| = \left|\left(e^{i\theta}\frac{gu_0}{||gu_0||}, e^{i\theta}\frac{gu_0}{||gu_0||}\right)\right| = \frac{|e^{i2\theta}|}{||gu_0||^2}|(u_0,u_0)| = \frac{\sqrt{cos^2 2\theta + sen^2 2\theta}}{||gu_0||^2} = \frac{1}{||gu_0||^2}.$$

Então, maximizar ϕ na esfera unitária equivale a minimizar a norma de Gu_0. O teorema enunciado acima implica que este subconjunto de elementos de Gu_0 que tem norma mínima é Ku_0, que é de fato a órbita de u_0.

Portanto temos que $\phi(w) = 1$ se e somente se w está na órbita de u_0. Isso completa a prova da propriedade.

Capítulo 7

Conclusão

A maior parte da segurança na internet se utiliza de algoritmos de criptografia, que se baseia no fato de que a fatoração de inteiros e que encontrar logaritmos discretos é extremamente difícil, já que não existem algoritmos eficientes para a solução destes problemas. Assim, a computação quântica atraiu muita atenção quando demonstrou-se que em um computador quântico esses problemas são resolvidos com complexidade polinomial, ou seja, são resolvidos de maneira eficiente. Com isso, este tema passou a ser amplamente estudado e desenvolvido, o que faz com que a área da computação quântica esteja muito ativa atualmente e em constante construção. Então, ter contato com este tema foi surpreendente e desafiador, já que por ser relativamente novo suas ideias ainda não são popularmente conhecidas e suas bases ainda não são tão profundas.

Embora o campo da computação quântica esteja bastante aquecido, ainda é necessário muito esforço e desenvolvimento para que a base teórica se torne mais sólida e para que vários problemas e obstáculos sejam solucionados ou minimizados.

Conforme já citado no texto, lidar com a imprecisão e a decoerência são problemas que dificultam a construção de um computador quântico. Apesar de já existirem códigos razoáveis para correção de erros [7], construir um computador quântico com precisão alta o suficiente e baixa taxa de decoerência para executar algoritmos com muitos passos, significa se deparar com dificuldades enormes.

O código para correção de erros descrito neste trabalho e outros presentes nas referências bibliográficas são construídos com base em simplificações e, portanto, possuem limitações. Além disso, a técnica usada para a construção destes códigos, conhecidos como códigos de repetição, que como o nome já diz geram redundância de dados, são bastante ineficientes na computação clássica [4]. Logo, existe um esforço para tornar os códigos para correção de erros mais abrangentes e eficientes. Esse esforço inclui não só o desenvolvimento dos algoritmos em si, mas também um estudo da mecânica quântica, para que se torne mais concreto o domínio de medições realizáveis em sistemas quânticos.

Além de pesquisadores e estudiosos da área, que se dedicam ao estudo da mecânica e computação quântica em universidades do mundo todo, alguns laboratórios também in-

vestem em pesquisas nesse campo, como o AT&T Bell Laboratories, que investe em pesquisa e desenvolvimento de tecnologias, e o Laboratório Nacional de Los Alamos, pertencente ao Departamento de Energia dos Estados Unidos, que conta com cientistas e estudantes desenvolvendo projetos científicos. Alguns dos artigos estudados para a redação deste trabalho foram escritos por profissionais atuantes nestes laboratórios.

Em 1999, o MIT, Massachusetts Institute of Technology, criou um protótipo de computador quântico, que contava apenas com 4 qubits. O experimento gerado no protótipo foi extremamente simples, já que o computador quântico era muito simplório e possuía menos poder de cálculo do que uma calculadora comum. Entretanto, este experimento mostrou que existe potencial para a construção de um computador quântico [14].

Em 2007, a empresa canadense D-Wave Systems anunciou a criação de um computador chamado Orion capaz de desempenhar operações quânticas. A comunidade científica recebeu a notícia com ceticismo, pois a D-Wave não forneceu nenhum detalhe sobre como o suposto processador quântico funciona e, além disso, os resultados de procedimentos realizados pelo Orion se mostraram mais lentos do que resultados obtidos em computadores clássicos utilizando-se dos melhores algoritmos conhecidos, o que implica que o Orion é extremamente mais lento do que o esperado para um computador quântico.

Apesar de todas as críticas recebidas por parte da comunidade científica, a D-Wave continua anunciando a evolução de suas experiências quânticas, ainda sem muitos detalhes, e tem recebido investimentos e clientes, como a empresa Lockheed Martin, que, em maio de 2011, assinou um acordo para a compra de um computador quântico [15].

O principal artigo estudado para a elaboração deste trabalho é voltado a matemáticos, especialmente em seus últimos dois capítulos onde se faz uso da teoria da Lie aplicada à computação quântica. A teoria de Lie é usada para identificar estados emaranhados, discriminar suas órbitas e gerar medidas de emaranhados. No penúltimo capítulo do artigo o autor apresenta medidas de emaranhados para qubits de tamanhos 2 e 3 e, no último, para qubits de tamanho 4 ou mais. Neste trabalho nos limitamos aos qubits de tamanho 2 e não mostramos como determinar um grupo gerador de medidas de emaranhados. Logo, esses são temas à serem abordados em trabalhos futuros.

Referências Bibliográficas

[1] WALLACH, Nolan R. **Quantum computing and entanglement for mathematicians**. In: C.I.M.E summer school in representation theory, 2004, Venice-Italy.

[2] PIZA, Antônio Fernando Ribeiro de Toledo. **Mecânica Quântica**. São Paulo: Editora da Universidade de São Paulo, 2003.

[3] SHOR, Peter W. **Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer**. In: SIAM J. Computing, 1997, USA.

[4] SHOR, Peter W. **Scheme for reducing decoherence in quantum computer memory**. In: Physical Review A, 1995, USA.

[5] GROVER, Lov K. **Quantum Mechanics helps in searching for a needle in a haystack**. In: Bell Labs, 1997, USA.

[6] KNILL, Emanuel; LAFLAMME, Raymond. **A Theory of Quantum Error-Correcting Codes**. In: Los Alamos National Laboratory, 1995, USA.

[7] LAFLAMME, Reymond et al. **Perfect Quantum Error Correcting Code**. In: Los Alamos National Laboratory, 2008, USA.

[8] HIRVENSALO, Mika. **Quantum Computing**. Springer, 2001.

[9] MUTHUKRISHNAN, Ashok. **Classical and Quantum Logic Gates: An Introdution to Quantum Computing**. In: Rochester Center for Quantum Information (RCQI), 1999, USA.

[10] QUANTIKI Wiki. **Encyclopedia of quantum information**. Disponível em: http://www.quantiki.org/wiki. Acesso em: 1 dez. 2011.

[11] LANG, Serge. **Undergraduate Analysis**. 2. ed. Springer, 2005.

[12] FRALEIGH, John B. **A First Course in Abstract Algebra**. 7. ed. Addison Wesley, 2003.

[13] KNAPP, Anthony W. **Lie Groups Beyond an Introdution**. 2. ed. Birkhäuser, 2002.

[14] MIT News. **MIT researchers create quantum computer that simulates quantum system**. Disponível em: http://web.mit.edu/newsoffice/1999/quantum.html. Acesso em: 17 out. 2011.

[15] D-WAVE, Press Releases. **D-Wave Systems sells its first Quantum Computing System to Lockheed Martin Corporation**. Disponível em: http://www.dwavesys.com/en/pressreleases.html. Acessado em 17 out. 2011.