Flávio Luís Alves

Computação Quântica: Fundamentos Físicos e Perspectivas

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do Curso de Ciência da Computação, para obtenção do título de Bacharel.

Orientador
Prof. Antonio Tavares da Costa Júnior

Lavras
Minas Gerais - Brasil
2003

Flávio Luís Alves

Computação Quântica: Fundamentos Físicos e Perspectivas

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do Curso de Ciência da Computação, para obtenção do título de Bacharel.

Avaliada em *10 / 12 / 2003*

Fortunato Silva de Menezes

Heitor Augustus Xavier Costa

Prof. Antonio Tavares da Costa Júnior
(Orientador)

Lavras
Minas Gerais - Brasil

Sumário

Dedico esta monografia à minha mãe e a meus irmãos

Agradecimentos

Ao professor Antonio Tavares da Costa Júnior que me ajudou imensamente durante todo o trabalho.
Aos professores Fortunato Silva de Menezes e Heitor Augustus Xavier Costa pelas valorosas sugestões para a correção final da monografia.
A Anderson de Rezende Rocha pelo imenso apoio e colaboração durante o desenvolvimento do projeto.
A Adriano Adriano Arlei de Carvalho, que me ajudou imensamente na implementação do simulador.
A todos os meus colegas que me acompanharam durante todo o curso.

Resumo

Computação Quântica: Fundamentos Físicos e Perspectivas

O interesse na Computação Quântica surge devido ao avanço de técnicas de manipulações de sistemas nanoscópicos. Avanço esse que proporcionou que idéias de manipulação quântica de informação pudessem ser implementadas, inicialmente apenas em nível de laboratório. Procuraremos aqui dar uma visão geral, e logo a seguir um embasamento teórico que está por trás do *Processamento Quântico*.

Capítulo 1

Introdução

Como todas as simples, mas profundas, idéias na ciência, levou tempo para que se notasse a conexão entre os conceitos de informação e computação e as propriedades de sistemas físicos microscópicos, propriedades como emaranhamento e superposição coerentes de estados distintos estão presentes nos fundamentos da mecânica quântica, e sempre foram considerados aspectos mais estranhos desta teoria.

O reconhecimento de que a informação, muito mais que um conceito matemático abstrato, é uma propriedade de sistemas físicos, levou a enormes avanços na interpretação conceitual da Mecânica Quântica.

Com a utilização da *Computação Quântica* a redução de tempo necessário para executar certas tarefas é de tal ordem que alguns problemas que levariam tempos impraticáveis em supercomputadores podem ser resolvidos em tempos normais em computadores quânticos, ou seja, problemas praticamente insolúveis para computação clássica passam a ser solúveis em computação quântica.

1.1 Mecânica quântica

A teoria quântica é, sem dúvida, o maior avanço da física no século XX, tendo representado o que se costuma chamar de uma revolução científica. Ao contrário da Mecânica Clássica, a Mecânica quântica possui características intrinsicamente probabilísticas.

Esta indeterminação é diferente daquela que surge na Mecânica Estatística Clássica, que é proveniente de um conhecimento incompleto sobre o sistema em questão. Um sistema quântico é probalístico intrinsicamente, ou seja, não existe

nenhuma variável que desconhecemos, o fato é que próprio sistema não “sabe” o valor das grandezas físicas a ele associadas.

Coloquialmente costuma-se descrever a Mecânica Quântica como uma teoria na qual nada é o que parece, ou o que o senso comum ou a física de Newton levam a acreditar. As coisas mudam quando se olha para elas. Os objetos se comportam de modo imprevisível. De acordo com o princípio da incerteza, que emerge da teoria quântica, nada pode ser medido tão precisamente quanto se deseja, pois o simples fato de medir afeta o estado daquilo que se mede.

Toda essa “estranheza” pode ser formulada precisamente, com base numa estrutura matemática coerente e extremamente elegante, como veremos mais tarde.

Da teoria quântica ainda surge o princípio da dualidade partícula-onda. Segundo este princípio, um elétron, por exemplo, pode comportar-se como partícula e as vezes como onda.

Por outro lado, toda onda possui uma partícula associada. O físico Richard Feynman usava um bom exemplo para explicar esta questão. Imagine luz sendo refletida por um espelho. Nenhum espelho é perfeito, deste modo apenas 95 % desta luz é refletida pelo espelho e os outros 5% o atravessam, ou é absorvido ou perdido.

Classicamente esta era uma situação completamente aceitável. Porém, sabe-se, da descoberta de Planck, que a luz é dividida em pacotes, ou quanta, chamados fótons. Estes fótons são indivisíveis. Desta forma, um fóton deve ser completamente absorvido ou refletido. Não é possível que um fóton seja parcialmente refletido e parcialmente absorvido. Então, conclui-se que 19 fótons de 20 são refletidos pelo espelho e o outro é absorvido. Mas como saber qual é absorvido e quais são refletidos? Não é possível saber. Um fóton tem 95% de chance de ser refletido e 5% de chance de ser absorvido. Não há nenhuma regra ou propriedade secreta do fóton que possa predizer seu comportamento. A imprevisibilidade é inata.

1.2 Computação quântica

1.2.1 O que é computação quântica

Um computador quântico é em príncipio, um dispositivo que usa as leis da Mecânica Quântica para processar informação. A principal vantagem de um computador quântico é o chamado “paralelismo quântico”. Este é baseado numa das propriedades mais estranhas da Mecânica Quântica, a superposição coerente de estados distintos. Em vez de um-ou-outro, como na lógica digital, um bit quântico poderia ser ambos-e, ou seja, representar 0 e 1 ao mesmo tempo. Esses qubits

poderiam existir simultaneamente como uma combinação de todos os números de dois bits possíveis quando se têm dois qubits. Adicionando um terceiro qubit, pode-se ter a combinação de todos os números de três bits possíveis. Esse sistema cresce exponencialmente. Com isso, uma coleção de qubits poderia representar uma fileira de números ao mesmo tempo, e um computador quântico poderia processar toda uma entrada de dados simultaneamente.

1.2.2 História

O interesse pela computação quântica teve início quando Feynman apontou, em 1982, que os sistemas clássicos não seriam capazes de modelar eficientemente os sistemas quânticos e que estes só poderiam ser modelados utilizando outro sistema quântico. Feynman sugeriu que computadores baseados nas leis da mecânica quântica ao invés das leis da física clássica poderiam ser usados para modelar sistemas quânticos. Deutsch foi o primeiro a levantar o questionamento de uma real maior capacidade de processamento dos computadores quânticos em relação aos clássicos em 1985. Com esta questão, ele estendeu a teoria da computação e ainda mais com o desenvolvimento dos conceitos de um computador quântico universal e da máquina quântica de Turing [Deutsch (1985)]. Foi ele também o primeiro a publicar um algoritmo quântico, o Problema de Dois Bits de Deutsch, em 1989. Este algoritmo poderia responder se uma função é balanceada ou constante em apenas um passo, enquanto em computação clássica precisa de no mínimo dois. Até 1990, computação quântica era apenas uma curiosidade.

Isto só mudou quando, em 1994, Shor publicou o seu algoritmo quântico que resolve o problema de fatoração de números
inteiros grandes[Shor (1994)]. Com este algoritmo, um número seria fatorado muito mais rapidamente do que com máquinas clássicas e por isso ficou conhecido como "killer application". A fatoração de números grandes é a base de alguns sistemas de criptografia, como, o RSA (em homenagem a Ronald Rivest, Adi Shamir e Leonard Adelman, os primeiros a propor o método em 1978). Deste modo, o algoritmo de Shor passou a despertar interesse em vários setores da comunidade científica.

A partir desse interesse, surgiram outros algoritmos quânticos, tais como o algoritmo para logaritmos discretos de Shor, outro de fatoração de
Jozsa[Jozsa (1997)], entre outros. Enquanto o número de algoritmos quânticos crescia, os esforços no sentido de produzir um hardware quântico também aumentavam. Técnicas como ressonância nuclear magnética (NMR) e armadilha de íons são usadas com sucesso no desenvolvimento de sistemas com 3 e 5 qubits.

No Apêndice B são apresentados alguns do principais centros de pesquisa na área de *Computação Quântica*.

1.2.3 Aplicações

Na maioria dos esquemas atuais de criptografia, incluindo esquemas utilizados para enviar números de cartão de crédito e outras informações sensíveis pela Internet, um bisbilhoteiro pode decifrar o código de uma determinada mensagem simplesmente fatorando um número muito grande. A fatoração de números pequenos é trivial; crianças de escola primária aprendem que 12 = 2 x 2 x 3. Entretanto fatorar números grandes é um dos problemas mais difíceis na ciência da computação. Não importa quão inteligente seja o algoritmo, na realidade o tempo exigido para fatorar números cada vez maiores cresce exponencialmente. Vá além de algumas centenas de dígitos e mesmo a capacidade das máquinas mais modernas no mundo será superada. O tempo de fatoração excederá o tempo de existência do universo. Ou melhor, isso aconteceria com um computador convencional.

Shor provou que um computador quântico poderia fatorar números grandes num prazo que aumenta somente algumas potências do tamanho do número. Crescimento rápido, certamente, mas nem tanto. Um computador convencional precisaria rodar por bilhões de anos para fatorar um número de 400 dígitos. Uma máquina quântica poderia fazer o serviço em cerca de um ano. A implicação era que códigos "indecifráveis"poderiam ser agora decifrados. e com este anúncio a Agência de Segurança Nacional, o Pentágono, a comunidade de criptografia e toda a comunidade de computação acordaram para o fato de que a computação quântica não era mais um domínio exclusivo dos teóricos. Peter Shor estava mostrando a possibilidade de uma aplicação real e importante.

1.3 Motivação

Desde muito novo, eu sempre gostei de física, principalmente astronomia. Cheguei a iniciar do curso de fisica na UFMG(Universidade Federal de Minas Gerais). Eu já havia tido contato com computação quântica quando eu estudava na UFMG. Mas na época tal tal teoria não passava de especulação científicas.

Há aproximadamente um ano, eu comecei a ler vários artigos sobre o tema. E isso despertou em mim um interesse de estudar o assunto, pois aliava mecânica quântica e computação, ciências que eu sempre admirei.

O tema é muitíssimo interessante e além disso talvez estejamos, em matéria

de tecnologia, em frente à maior descoberta de todos os tempos; talvez, em frente a uma tecnologia de dificílima implementação que pode cair no esquecimento. O fato é que, hoje, essa tecnologia pode ser inegavelmente considerada revolucionária, já que começou-se a demonstrar a possibilidade de solução para problemas de alta complexidade, o que computadores digitais clássicos não fariam. Quando entramos no mundo da computação quântica e conseqüentemente da física quântica, temos, no entanto, encontrado mais problemas do que soluções. Estamos na pré-história da computação quântica, e a idéia de supercomputadores, ou mesmo laptops quânticos é uma fantasia infinitamente distante Não há como negar entretanto, que foi dado o primeiro passo.

1.4 Objetivos

Nesta monografia foram abordados os principais fundamentos teóricos que estão por trás da *Computação Quântica*. Foram apresentados todos os aspectos importantes da *Mecânica Quântica*: seus principais postulados e outras partes que são importantes para o entendimento do funcionamento do processamento quântico. E também como essa teoria é aplicada no desenvolvimento do *Computador Quântico*. Será apresentado o que há de mais recente na *Computação Quântica*, como: os algoritmos já desenvolvidos, as aplicações e as perspectivas de futuro para essa tecnologia. Durante o projeto desenvolvemos um simulador de evolução temporal de um sistema quântico de dois niveis, a base para o desenvolvimento de qualquer algoritmo quântico.

1.5 Descrição do conteúdo da monografia

A monografia é dividida em 7 capitulos, além de dois apêndices. Uma breve descrição é apresentada a seguir:

Capítulo 1 - Introdução Neste capitulo apresentaremos uma breve descrição informal do que é a mecanica quântica. Logo em seguida apresentaremos o conceito de computação quântica, seus aspectos históricos e aplicações.

Capitulo 2 - Breve introdução à mecânica quântica Aqui abordadoremos os aspectos mais formais da mecânica quântica: como por exemplo os postulados e ferramentas matemáticas.

Capítulo 3 - Implementação dos computadores quânticos Neste capítulo apresentaremos as principais abordagens para a implementação dos computadores quânticos.

Capitulo 4 - Metodologia Aqui apresentados os métodos utilizados para o desenvolvimento do projeto

Capítulo 5 - Evolução temporal e medida de um qubit Apresentaremos aqui os resultados da evolução temporal e discutiremos os resultados.

Capítulo 6 - Conclusões Discutiremos aqui os resultados da pesquisa os resultados obtidos durante o projeto.

Capítulo 7 - Referências bibliográficas Apresentaremos neste capítulo as referência bibliográficas utilizadas.

Apêndice A - Suplemento Matemático Neste apêndice apresentaremos alguns aspectos mais formais da estrutura matemática da mecânica quântica.

Apêndice B - Centros de pesquisa Neste apêndice apresentaremos os principais centros de pesquisa na área de computação quântica.

Capítulo 2

Breve introdução à mecânica quântica

A mecânica quântica é a teoria que descreve corretamente o comportamento físico de sistemas microscópicos, como átomos e moléculas. Qualquer sistema com tamanho na escala dos Angstrons (1 Å = 10^{-10}m) sofre a influência de efeitos quânticos.

2.1 Estado

Um estado de um sistema clássico (governado pela mecânica newtoniana) é caracterizado por valores bem definidos das grandezas físicas mensuráveis. Posição, velocidade, energia, todas têm valores bem definidos a todo instante. Determinar o estado de um sistema quântico corresponde a especificar probabilidades de encontrar determinados valores para as grandezas físicas mensuráveis. Existe uma incerteza intrínseca ao sistema. Essa incerteza é descrita matematicamente como uma superposição coerente de estados distintos. Essa superposição corresponderia, grosso modo, ao sistema estar, ao mesmo tempo, em vários estados clássicos diferentes. O estado clássico de uma partícula é representado matematicamente por um ponto no espaço de fases, formado pelas componentes da posição e da velocidade da partícula. Na mecânica quântica, o estado de uma partícula é representado matematicamente por um vetor num espaço vetorial complexo, chamado espaço de Hilbert.

Para descrever esta situação pouco usual com precisão, necessitamos de ferramentas matemáticas diferentes daquelas usadas na mecânica clássica. Vamos

apresentar agora, brevemente, a estrutura matemática por trás da mecânica quântica.

2.2 Espaço de Hilbert

O Espaço de Hilbert é um espaço vetorial $\mathcal{H}$, definido sobre o conjunto dos números complexos, sendo assim, satisfaz as seguintes propriedades:

1. $\mathcal{H}$ é um conjunto de objetos chamados vetores, com uma operação de soma de vetores definida de tal forma que:

   i) se dois vetores $|f\rangle, |g\rangle \in \mathcal{H}$, então a soma $|f\rangle + |g\rangle$ também é um vetor de $\mathcal{H}$;

   ii) a soma é comutativa e associativa: $|f\rangle + |g\rangle = |g\rangle + |f\rangle$ e $(|f\rangle + |g\rangle) + |h\rangle = |f\rangle + (|g\rangle + |h\rangle)$

   iii) existe em $\mathcal{H}$ um vetor chamado nulo, tal que $|f\rangle + 0 = |f\rangle \; \forall |f\rangle \in \mathcal{H}$

   iv) Também está definida uma operação de produto por escalar de tal forma que, se $\alpha,\ \beta$ pertencem ao conjunto dos complexos, e $|f\rangle$ e $|g\rangle$ são elementos de $\mathcal{H}$, então:

   (a) $\alpha|f\rangle \in \mathcal{H}$
   (b) $(\alpha\beta)|f\rangle = \alpha(\beta|f\rangle)$
   (c) $(\alpha + \beta)|f\rangle = \alpha|f\rangle + \beta|f\rangle$
   (d) $\alpha(|f\rangle + |g\rangle) = \alpha|f\rangle + \alpha|g\rangle$
   (e) $1.|f\rangle = |f\rangle$

2. $\mathcal{H}$ tem um produto interno, ou seja, pode-se definir uma operação entre dois vetores $|f\rangle$ e $|g\rangle$ de $\mathcal{H}$ que fornece um escalar, denotada por $(|f\rangle,\ |g\rangle)$, que possui as seguintes propriedades:

   i) $(|f\rangle,\ |g\rangle) = (|g\rangle,\ |f\rangle)^*$

   ii) $(|f\rangle,\ |g\rangle + |h\rangle) = (|f\rangle,\ |g\rangle) + (|f\rangle,\ |h\rangle)$

   iii) $(|f\rangle, \alpha|g\rangle) = \alpha(|f\rangle, |g\rangle)$

   iv) $(\alpha|f\rangle,\ |g\rangle) = \alpha^*(|f\rangle,\ |g\rangle)$

   v) $(|f\rangle,\ |f\rangle) \geq 0$, e $(|f\rangle,\ |f\rangle) = 0$ se e somente se $|f\rangle = 0$ (vetor nulo).

Usa-se com bastante frequência uma notação mais conveniente para o produto interno $(|f\rangle,\ |g\rangle) \equiv \langle f|g\rangle$. Esta notação está baseada na definição de um espaço vetorial dual de $\mathcal{H}$. Esta construção matemática é um pouco mais formal, e não é essencial à compreensão do que se segue. Deixamos, portanto, sua exposicao para o apêndice A.

A existência do produto interno em $\mathcal{H}$ dota o espaço de uma noção natural de distância. Diz-se então que $\mathcal{H}$ é um espaço métrico. Definimos a norma de um vetor de $\mathcal{H}$ por $\||f\rangle\| = \sqrt{\langle f|f\rangle}$.

Dados dois vetores x e y em um Espaço de Hilbert $\mathcal{H}$, diz-se que são ortogonais se seu produto interno é zero, ou seja,

$$\langle x|y\rangle = 0 \Rightarrow |x\rangle \perp |y\rangle.$$

Uma base de $\mathcal{H}$ é o menor subconjunto $\{|e_1\rangle, |e_2\rangle, ...|e_N\rangle\}$ de $\mathcal{H}$ que varre o espaço todo, ou seja, qualquer vetor de $\mathcal{H}$ pode ser escrito como uma combinação linear dos vetores deste conjunto:

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i |e_i\rangle \tag{2.1}$$

Dizemos que N é a dimensão de $\mathcal{H}$. Se este conjunto for ortonormal, dizemos que ele é uma base ortonormal de $\mathcal{H}$. Bases ortonormais sao muito convenientes para expressar vetores de $\mathcal{H}$.

2.3 Observáveis

Na mecânica quântica, quantidades mensuráveis estão associadas a um tipo especial de operadores lineares que atuam sobre vetores do espaço de estados $\mathcal{H}$. Esses operadores são chamados observáveis. Para definir um observável, precisamos primeiro definir o que é um operador, e depois o que é o hermiteano conjugado de um operador.

Um operador A é um mapa linear entre dois espaços de Hilbert. Para a mecânica quântica são importantes os operadores lineares que mapeiam o espaço de estados $\mathcal{H}$ no proprio $\mathcal{H}$. Representamos a atuação de um operador A na forma de "produto":

$$\begin{aligned} A : \mathcal{H} &\rightarrow \mathcal{H} \\ |f\rangle &\rightarrow |g\rangle = A|f\rangle \end{aligned}$$

Podemos definir o hermiteano conjugado de um operador A da seguinte forma: Se $A|f\rangle = |g\rangle$, $\langle g|h\rangle = \langle f|A^\dagger|h\rangle$, e $A^\dagger$ é chamado o hermiteano conjugado de A.

Um operador será um observável se ele for auto-adjunto, ou seja, $A^\dagger = A$. Esta propriedade faz com que os auto-valores de $\mathcal{H}$ sejam todos reais. Como os resultados possíveis de uma medida são os autovalores do operador A associado à quantidade medida, é de se esperar que operadores associados à quantidades fisicas tenham apenas autovalores reais, que é uma das propriedades dos operadores auto-adjuntos.

2.4 Medições

Uma outra propriedade importante dos operadores auto-adjuntos é que seus autovetores formam um conjunto ortogonal, que fornece uma base ortonormal para $\mathcal{H}$[1]. Sendo assim, é sempre possível escrever um estado qualquer de um sistema quântico em termos dos autovetores de um observável A. Sejam então $\{|a_1\rangle, |a_2\rangle, ...|a_N\rangle\}$ os autovetores de A, associados aos autovalores $\{a_1, a_2, ...a_N\}$. Se o sistema está num estado qualquer $|\psi\rangle$, sempre podemos escrever $|\psi\rangle = \sum_{i=1}^{N} \alpha_i |a_i\rangle$. Um dos postulados da mecânica quântica diz que, se fizermos um experimento para medir qual valor da grandeza física associada ao operador A que o sistema possui quando está no estado $|\psi\rangle$, encontraremos o autovalor a_l com probabilidade $\|\alpha_l\|^2$. Um outro postulado afirma que, após uma medida, o estado do sistema passa a ser descrito pelo autoestado de A associado ao autovalor que foi o resultado da medida. Este fato é conhecido como o "colapso do estado quântico". Se novas medidas de A forem feitas, os resultados serão sempre a_l, com probabilidade 1.

2.5 Hamiltoniano

O hamiltoniano é um operador especial. Ele é o observável associado à energia total do sistema quântico. Sendo assim, seus autovalores são os valores possíveis (ou permitidos) para a energia do sistema. O fato de que os hamiltonianos de vários sistemas fisicos apresentam um conjunto discreto de autovalores é a manifestação matemática da quantização de energia.

O papel do hamiltoniano é ainda mais importante do que fornecer os valores permitidos de energia do sistema. Ele determina, através da equação de Scrödin-

[1] A forma precisa desta afirmacao esta descrita no apêndice A

ger, a maneira como o sistema quântico evolui no tempo. A equação de Scrhödinger pode ser escrita como

$$H|\psi(t)\rangle = -i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle \tag{2.2}$$

Mostra-se que a solução desta equação pode ser escrita como o resultado da aplicacao de um operador linear (chamado de operador de evolução temporal) $U(t, t_0)$ sobre o estado inicial do sistema $|\psi(t_0)\rangle$, $|\psi(t) = U(t, t_0)|\psi(t_0)\rangle$.

Se o hamiltoniano do sistema nao depende explicitamente do tempo, o operador de evolucao temporal $U(t, t_0)$ é dado por:

$$U(t, t_0) = e^{\frac{-iH(t-t_0)}{\hbar}} \tag{2.3}$$

O significado matemático da exponencial de um operador está explicado no apêndice A.

É importante notar que a dinâmica quântica tem um caráter estritamente *determinístico*, ou seja, dado que o sistema encontra-se inicialmente num $|\psi(0)\rangle$, existe uma regra para determinar precisamente seu estado quântico $|\psi(t)\rangle$ em qualquer tempo posterior. O caráter probabilístico da mecânica quântica está no fato de que o estado quântico, em qualquer instante, fornece apenas probabilidades de encontrar-se em um determinado valor para uma determinada quantidade física. Isto fica evidente no enunciado do postulado que diz respeito a medidas feitas num sistema quântico.

Outro aspecto importante da evolução temporal quântica é que ela é unitária, ou seja, a norma do vetor de estado é constante no tempo. Isso resulta de uma propriedade matemática do operador de evolução temporal: $U^\dagger = U^{-1}$. Diz-se que U é um operador unitário.

2.6 Postulados da mecânica quântica

Embora já tenhamos mencionado alguns dos postulados da Mecânica Quântica, vamos sumarizá-los aqui para melhor compreensão.

Postulado 1

O estado de um sistema quântico é descrito por um vetor pertencente a um espaço de Hilbert.

Postulado 2

A cada grandeza física mensurável corresponde um operador linear hermiteano que atua sobre um espaço de Hilbert, chamado de observável.

Daqui por diante nos referiremos à grandeza física e ao seu observável associado indistintamente. Ficará sempre claro, pelo contexto, sobre qual dos dois estaremos falando.

Postulado 3

Os resultados possíveis de uma medição do observável G são os autovalores de G, ou seja as soluções da equação:

$$G|\phi_i\rangle = g_i|\phi_i\rangle \tag{2.4}$$

Postulado 4

Se $|\Psi(t)\rangle$ representa o estado quântico normalizado de um sistema no instante *t*, então o valor médio do observável *G* nesse instante é:

$$\langle G\rangle = \langle\Psi|G|\Psi\rangle \tag{2.5}$$

Postulado 5

A equação de Schrödinger é a equação fundamental da mecânica quântica, no mesmo sentido que a segunda lei do movimento constitui a equação fundamental da mecânica newtoniana. Ela nos dá a assistência necessária para conhecermos a forma do estado quântico $|\psi(t)\rangle$, caso seja conhecida a força que atua sobre a partícula associada, especificando a energia potencial correspondente. Em outras palavras, o estado quântico é uma solução da equação de Schrödinger para aquela energia potencial. De fato, a equação de Schrödinger é uma equação diferencial,

$$-i\hbar\frac{\partial|\Psi\rangle}{\partial t} = \hat{H}|\Psi\rangle, \tag{2.6}$$

Onde $H = T+V$, sendo T operador de energia cinética e V o operador de energia potencial do sistema.

2.7 Qubit

O bit é o conceito fundamental da computação clássica e da informação clássica. Ele pode assumir dois estados - 0 ou 1. Pode-se pensar num bit clássico como sendo um sistema físico clássico de dois níveis. A Computação Quântica e a Informação Quântica são construídas sobre um conceito análogo, o bit quântico, ou qubit. Ao contrário de seu análogo clássico, o bit quântico pode estar numa infinidade de estados, representados por superposições coerentes dos estados $|0\rangle$ e $|1\rangle$. Em outras palavras, um bit quântico é qualquer sistema quântico de dois níveis. Dois possíveis estados para um qubit são os estados $|0\rangle$ e $|1\rangle$. O estado de um qubit pode ser representada por uma combinação linear de estados, chamada superposição coerente:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.7}$$

Os números α e β são números complexos. O estado de um qubit é um vetor num espaço de Hilbert de duas dimensões. Os estados especiais $|0\rangle$ e $|1\rangle$ formam uma base ortonormal para para o espaço de estados.

Os estados $|0\rangle$ e $|1\rangle$ são autoestados de algum observável do sistema quântico de dois níveis que escolhemos para representar o qubit. Por conveniência, e para manter compatibilidade com a linguagem normalmente usada em computação, dizemos que os autovalores associados a esses dois estados são 0 e 1, respectivamente.

Quando é feita a medida medida deste observável é possível encontrar ou o valor 0, com probabilidade $|\alpha|^2$ ou o valor 1, com probabilidade $|\beta|^2$. Naturalmente $|\alpha|^2 + |\beta|^2 = 1$, pois a soma das probabilidades deve ser igual a um. Além disso, exceto quando $\alpha = 0$ ou $\beta = 0$ a medida causa distúrbios no estado. Mais uma diferença entre os bits clássicos e os qubits é que os bits clássicos podem ser medidos e manipulados sem sofrerem distúrbios.

2.8 Paralelismo quântico

É a principal vantagem dos computadores quânticos em relação aos computadores clássicos. O paralelismo quântico permite aos computadores quânticos avaliarem uma função $f_(x)$ para muitos valores diferentes de x simultaneamente.

Devido ao chamado paralelismo quântico, a computação quântica promete uma revolução na maneira de lidar problemas comumente intratáveis na computação clássica. O funcionamento dos componentes dos computadores atuais é

baseado nas propriedades quânticas da matéria, contudo, os bits, unidades fundamentais de processamento, são clássicos, dado que podem estar apenas no estado $|0\rangle$ ou no estado $|1\rangle$. Em contraposição, os bits de um computador quântico, ou quBits, poderiam ser colocados em estados que são superposições coerentes do estado $|0\rangle$ e do estado $|1\rangle$.

Suponha que $f_{(x)} : \{0, 1\} \rightarrow \{0, 1\}$ seja uma função que mapeia um único bit x para um unico bit $f_{(x)}$.

Um modo conveniente de computar esta função em um computador quântico é considerar um computador quântico de dois dois qubits que começa no estado $|x, y\rangle$. Com uma apropriada sequência de portas lógicas é possível transformar este estado em $|x, y \oplus f_{(x)}\rangle$, onde $\oplus$ indica adição módulo 2; o primeiro registrador é chamado de registrador de dados , e o segundo registrador de registrador alvo. A transformação U_f é definida como:

$$|x, y\rangle \rightarrow |x, y \oplus f_{(x)}\rangle, \tag{2.8}$$

e é fácil notar que é uma transformação unitária. Se $y = 0$, então o estado final do segundo qubit é apenas $f_{(x)}$.

Se aplicarmos U_f às entradas $x = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $y = |0\rangle$ obteremos o seguinte estado:

$$\frac{|0,\ f_{(0)}\rangle + |1,\ f_{(1)}\rangle}{\sqrt{2}} \tag{2.9}$$

X é preparado aplicando-se a porta Hamadard[2] a entrada $|0\rangle$.

Este é um estado extraordinário! Os diferentes termos contém informação sobre $f_{(0)}$ e $f_{(1)}$; é como se tivéssemos avaliado $f_{(x)}$ para dois valores de x simultaneamente, uma característica conhecida como paralelismo quântico. Diferente do paralelismo clássico, onde múltiplos circuitos, cada um construído para computar $f_{(x)}$, são executados simultaneamente, aqui um único circuito $f_{(x)}$ é empregado para avaliar a função para múltiplos valores de x ao mesmo tempo, ao explorar a habilidade de um computador quântico para estar em superposições de diferentes estados.

Este procedimento pode facilmente ser generalizado para funções em um número arbitrário de bits, ao usar uma operação geral conhecida como a *transformada de Hamadard*, ou algumas vezes como *transformada de Walsh-Hamadard*.

[2] A porta Hamadard é definida como:

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

.

Esta operação é apenas n portas Hamadard agindo em paralelo em n qubits. Nós escrevemos $H^{\oplus 2}$ para denotar a ação paralela de de duas portas Hamadard, e $\oplus$ deve ser lido como produto tensorial[3]. Mais geralmente, o resultado de processar a transformada de Hamadard em n qubits, todos inicialmente no estado $|0\rangle$ é:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle, \tag{2.10}$$

onde a soma é sobre sobre todos os valores possíveis de x, e escreve-se $H^{\oplus n}$ para denotar esta ação. Isso é, a transformada de Hamadard produz uma superposição uniforme de todos os estados da base computacional: $\{|0\rangle, |1\rangle\}$. Além disso, faz isto de modo extremamente eficiente, produzindo uma superposição de 2^n estados usando apenas n portas.

A evolução paralela quântica de uma função com uma entrada de n bits x e uma saída de um bit, $f_{(x)}$, pode então ser preparada da seguinte maneira: prepara-se os $n+1$ estados do qubit $|0\rangle^{\oplus}|0\rangle$, então aplica-se a transformada de Hamadard para os n primeiros qubits em seguida aplica-se U_f. Isto produz o estado:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f_{(x)}\rangle. \tag{2.11}$$

O paralelismo quântico possibilita que todos os valores de uma função f sejam avaliados simultaneamente, sendo que f é avaliado apenas uma vez. Contudo este paralelismo não é imediatamente útil. Para o caso do qubit dado como exemplo, a medida dá somente $|0,\ f_{(0)}\rangle$ ou $|1,\ f_{(1)}\rangle$! Similarmente, no caso geral a medida do estado $\sum_x |x\rangle|f_{(x)}\rangle$ dá somente $f_{(x)}$ para um único valor de x. A computação quântica requer alguma coisa mais do que paralelismos quântico para ser útil; ela requer a habilidade para extrair a informação sobre mais de um valor de $f_{(x)}$ da superposição $\sum_x |x\rangle|f_{(x)}\rangle$. É necessária, então a elaboração de algoritmos quânticos que aproveitem o paralelismo. Estes algoritmos correspondem a um conjunto de operações unitárias aplicadas sobre os qubits da computação quântica, seguidas por medidas de observáveis cuidadosamente escolhidos.

2.8.1 O algoritmo de Deutsch

David Deutsch[Nielsen e Chuang, 2000] deu um exemplo concreto sobre as possibilidades e vantagens de um computador quântico, em 1985. Deutsch enfa-

[3]Ver Apêndice A

tizou que um computador quântico poderia realizar melhor seu potencial computacional se utilizasse o chamado paralelismo quântico. Para entender o que isso significa, considere o exemplo a seguir.

Seguindo a idéia de Deutsch, imagine que se tenha uma caixa preta que computa uma função que mapeia um simples bit x para um simples bit $f(x)$. Não se conhece o que ocorre dentro da caixa, mas suponha algo complicado o suficiente para que sua computação consuma 24 horas. Há quatro possibilidades de funções para $f(x)$ pois $f(0)$ pode ser 0 ou 1 e, por sua vez, $f(1)$ pode, também, ser 0 ou 1. Não se sabe o valor que a caixa preta está computando. Logo, gasta-se 48 horas para que $f(0)$ e $f(1)$ sejam calculadas.

Suponha, agora, que o objetivo seja saber se $f(x)$ é constante com $f(0) = f(1)$ ou balanceada com $f(0) \neq f(1)$. Considere agora que não se tenha 48 horas disponíveis para tal atingir tal objetivo; precisa-se de uma resposta em 24 horas.

Agora suponha que se tenha uma caixa preta quântica capaz de computar $f(x)$. De fato, $f(x)$ pode não ser uma função inversível, enquanto a ação deste computador quântico é unitária e precisa ser inversível. Assim, é preciso uma transformação Uf que leve 2 quBits em outros dois quBits:

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_{(x)}\rangle. \tag{2.12}$$

A operação $y \oplus f_{(x)}$ é a operação de xor binária.

Esta máquina troca o segundo quBit se f atua no quBit 1 resulta em 1 e se f atua no quBit 2 resulta em 0. Claramente, pode-se concluir que a a função $f(x)$ é constante ou balanceada utilizando-se a caixa-preta duas vezes. Mas isto ainda tomaria 48 horas para fazê-lo. Logo, isto não será feito. Este é o problema de Deutsch.

Pelo fato de a caixa preta ser um computador quântico, pode-se escolher a entrada como sendo uma superposição de $|0\rangle$ e $|1\rangle$. Se o segundo quBit for inicialmente preparado no estado: $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, então:

$$\begin{aligned} U_f : |x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \;\rightarrow\; |x\rangle\frac{1}{\sqrt{2}}(|f_{(x)}\rangle - |1 \oplus\; f_{(x)}\rangle) \\ = |x\rangle(-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Deste modo, isolou-se a função f em uma fase dependente de x. Agora suponha que o primeiro quBit tenha sido preparado no estado: $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Então a caixa preta atuará como:

$$U_f : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\ \rightarrow$$
$$\frac{1}{\sqrt{2}}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Finalmente, pode-se fazer uma medida que projeta o primeiro quBit sobre a base:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

Evidentemente, sempre será obtido $|+\rangle$ se a função é balanceada, e $|-\rangle$ se a função é constante [4]. Com esta abordagem o problema de Deutsch foi resolvido e agora é possível fazer uma separação entre o que os computadores clássicos e os quânticos podem atingir. Um computador clássico precisa executar a caixa preta duas vezes para comparar duas funções unárias e classificá-las como contantes ou balanceadas. Por outro lado, um computador quântico faz a mesma tarefa em apenas um passo. Realmente um ganho considerável. Isto é possível porque os computadores quânticos não são limitados a trabalhar com funções $f(0)$ ou $f(1)$. Eles podem atuar em uma superposição dos estados $\{|0\rangle$ e $|1\rangle\}$, e, através disso, extrair uma informação global sobre a função, informação esta que depende de $f(0)$ e $f(1)$ correlacionando-as. .

2.9 Decoerência

Os sistemas estudados não são, em geral, isolados. O maior problema para construir computadores do quânticos é a decoerência, a distorção do estado quântico devido à interação com o ambiente. A inevitável interação entre esses sistemas e o ambiente que os cerca tem como efeito a destruição das características quânticas classicamente ausentes dos fenômenos em questão.

[4] Geralmente a medida final de uma computação quântica projeta cada quBit sobre a base $\{|0\rangle, |1\rangle\}$. Entretanto, aqui foi permitido uma medida em uma base diferente. Para proceder como anteriormente, sem perda de generalidade, basta aplicar uma mudança unitária da base para cada quBit antes de fazer a medida final.

2.10 Spin do elétron

O spin é uma propriedade intrínseca de várias partículas subatômicas. Matematicamente, esta propriedade tem todas as características de um momento angular, embora não se possa associar a ela nenhum movimento real de rotação. O spin é um dos observáveis quânticos que não possui análogo clássico.

Ao momento angular de uma partícula carregada eletricamente está sempre associado um momento magnético, que é, no caso do spin, a maneira pela qual podemos detectar experimentalmente a presença deste momento angular.

O spin surge naturalmente na descrição quântica-relativística do elétron, representada matematicamente pela equação de Dirac [Dirac]. Na mecânica quântica não-relativística ele tem que ser introduzido *ad hoc*. Pauli desenvolveu uma teoria que permitiu que o spin fosse incorporado à Mecânica Quântica não-relativística através da introdução de vários postulados suplementares.

Evidências experimentais da existência do spin do elétron são numerosas e aparecem em vários fenômenos físicos importantes. Por exemplo, as propriedades magnéticas de várias subtâncias, particularmente de metais ferromagnéticos, podem somente ser explicadas se o spin do elétron for levado em conta.

Logo a seguir serão descritos alguns fenômenos observados experimentalmente em física atômica: a estrutura fina de linhas espectrais e o efeito Zeeman Anômalo.[Cohen, 1977]

A Estrutura fina das linhas espectrais

O hamiltoniano de um elétron num átomo, como o hidrogênio, por exemplo, é tal que os níveis de energia permitidos formam um conjunto discreto, separados por energias proibidas, e esta separação pode ser calculada a partir dos autovalores do hamiltoniano. Sendo assim, espera-se, a princípio, que uma medida espectroscópica revele linhas bem definidas, com a separação prevista pelo hamiltoniano do sistema. Entretanto, com aparelhos de boa resolução, é possível mostrar que as linhas previstas pelos autovalores do hamiltoniano sem spin subdividem-se em "sub-linhas", cujo espaçamento em energia é muito menor do que o espaçamento entre as linhas originais. A existência destas subdivisões é explicada pela existência do spin, e sua interação com o momento magnético orbital.

Efeito Zeeman

Quando um átomo é colocado em um campo magnético uniforme, cada um de seus níveis de energia, divide-se em dois níveis equidistantes em energia do nível original, sendo a distância proporcional ao campo magnético. Este fenômeno pode ser explicado supondo-se a existência do spin. Sabe-se que toda partícula que possui momento angular possui um momento magnético associado; no caso do elétron, o momento magnético associado ao spin é:

$$M = \frac{\mu_B}{\hbar} \tag{2.13}$$

onde μ_B é o "magneton" de Bohr:

$$\mu_B = \frac{q\hbar}{2m_e} \tag{2.14}$$

Este momento magnético interage com um campo magnético aplicado, de tal forma que a energia desta partícula depende da orientação do seu momento angular com relação ao campo magnético, daí a duplicação do número de níveis de energia."

O experimento de Stern-Gerlach

O experimento consiste em estudar a deflexão de um feixe de átomos paramagnéticos neutros (neste caso átomos de prata) em um campo magnético não-homogêneo. O aparato usado é mostrado na Figura 2.1.

Átomos de prata contidos em uma fornalha *E*, que é aquecida a alta temperatura, atravessam uma pequena abertura e propagam-se em linha reta em alto vácuo que existe dentro de todo o aparato. Uma fenda de observação *F* seleciona os átomos cuja velocidade é paralela a uma direção que nós escolheremos como sendo o eixo O_y. O feixe atômico então construído atravessa o vácuo de um eletromagneto *A* antes de se condensar em uma placa *P*.

Vamos descrever as características do campo magnético **B** produzido pelo eletromagneto *A*. Este campo magnético tem um plano de simetria (que nós designaremos por yOx) que contém a direção inicial O_y do feixe atômico. No vácuo ele é o mesmo em todos os pontos situados em qualquer linha paralela a O_y. **B** não tem nenhum componente em O_z. Seu maior componente é ao longo de O_x; ele varia fortemente com x.

No Experimento de Stern-Gerlach verificou-se que o feixe de átomos de prata é dividido simetricamente em dois. Estes resultados sugerem que j (momento

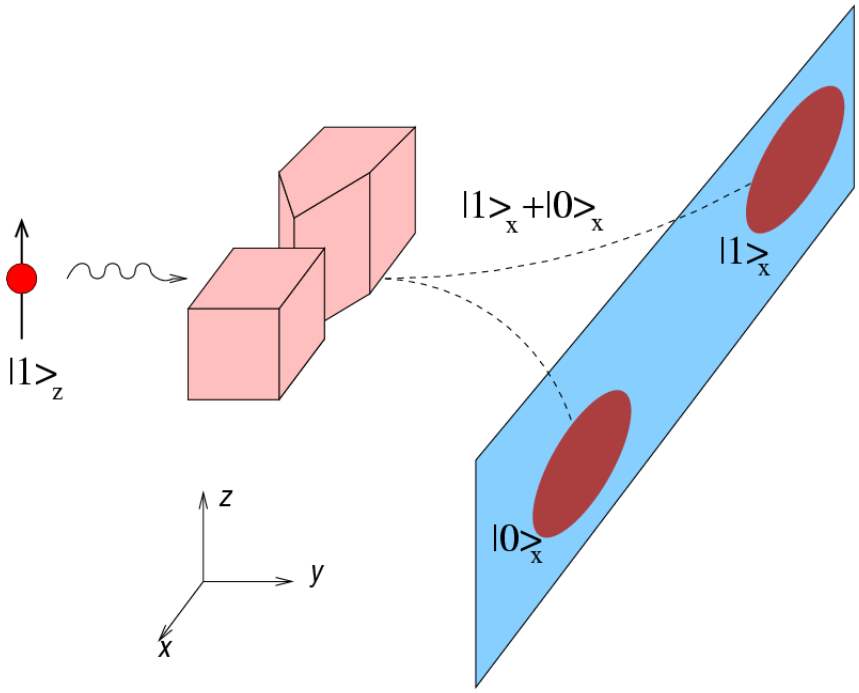

Figura 2.1: O experimento de Stern-Gerlach

angular orbital) pode assumir valores semi-inteiros. Mas a teoria afirmava que o momento angular orbital de uma partícula deveria somente ser inteiro. Até mesmo em átomos com vários elétrons, cada um destes tem um momento angular orbital inteiro. A existência de momento angular semi-inteiro não pode ser explicado com o auxílio de hipóteses suplementares.

2.10.1 O operador de spin

As evidências experimentais apontam, então, para a existência de um momento angular intrínseco ao elétron, chamado spin, que não está associado a nenhum movimento real de rotação. Este momento angular é uma grandeza física mensurável e, como tal, deve ter um observável associado. A idéia principal da formulação não-relativística do spin é que os oberváveis associados ao spin devem ter a mesma estrutura matemática do operador de momento angular orbital. Isso significa que, primeiro, o operador de spin deve ser um vetor de três componentes (todas opera-

dores), e essas componentes devem obedecer às seguintes relações de comutação:

$$[S_x,\ S_y] = i\hbar S_z, \tag{2.15}$$

e permutações cíclicas. Pode-se mostrar que um operador que obedece às relações de comutação acima pode possuir autovalores inteiros (n=1,2,...) ou semi-inteiros ((2n+1)/2, n=1,2,...). De fato, verifica-se que existem partículas cujo spin é inteiro, que são chamadas de bósons, e outras cujo spin é semi-inteiro (chamadas férmions). O elétron é um férmion, com spin 1/2; os valores possíveis do spin ao longo de uma dada direção no espaço são, portanto, $\pm 1/2$. Esta característica faz com que o spin do elétron seja um excelente candidato a qubit: ele é o protótipo de um sistema quântico de dois níveis. A estrutura matemática do espaço de estados de qualquer sistema de dois níveis é idêntica à do espaço de estados do spin eletrônico.

Capítulo 3

Implementação dos computadores quânticos

Vários estudos têm sido feitos no sentido de conseguir uma implementação plausível e útil de um computador quântico [Preskill, 2002].

Para se conseguir construir o *hardware* para um computador quântico, é necessário uma tecnologia que possibilite a manipulação de quBits. O *hardware* precisará se adequar a alguns requisitos severos:

- Armazenamento. Os quBits precisam ser armazenados por períodos de tempo suficientes para completar computações interessantes.
- Isolamento. Os quBits precisam estar isolados do ambiente, para minimizar erros por decoerência.
- Leitura. Os quBits precisam permitir sua leitura de forma eficiente e confiável.
- Portas lógicas. É necessário a possibilidade de manipulação de quBits individuais. Deste modo, para permitir interações controladas entre quBits é necessário a construção de portas lógicas quânticas.
- Precisão. As portas lógicas quânticas precisam ser implementadas com alta precisão se o dispositivo for para cálculos confiáveis.

A seguir serão apresentadas três abordagens para implementação de um computador quântico que estão sendo investigados presentemente.

3.1 Armadilha de íons

Um meio possível para atingir os requisitos citados foi proposto por Ignacio Cirac e Peter Zoller[CZ95] e tem sido continuado pelo grupo de pesquisas de Dave Wineland no *National Institute for Standards and Technology*, **NIST**, nos EUA[WMI$^+$]. Neste esquema, cada quBit é representado por um íon aprisionado em uma *armadilha linear* de Paul.

O estado quântico vibracional de cada íon é uma combinação linear do estado fundamental $|g\rangle$ (interpretado como $|0\rangle$) e um estado excitado metaestável (de longa duração) $|e\rangle$ (interpretado como $|1\rangle$). Uma combinação linear coerente destes dois níveis,

$$a|g\rangle + be^{iwt}|e\rangle, \tag{3.1}$$

pode sobreviver por um tempo comparável a uma vida inteira de um estado excitado (apesar de que as fases relativas oscilam devido à diferença de energia $\hbar\omega$ entre os níveis). Os íons são tão bem isolados que decaementos espontâneos podem ser a forma dominante de decoerência.

É relativamente fácil ler os íons através de sua medida que faz a projeção sobre a base $\{|g\rangle,\ |e\rangle\}$. Um laser é sintonizado para uma transição a partir do estado $|g\rangle$ para um estado excitado de vida curta $|e\prime\rangle$.

Quando o laser ilumina os íons, cada quBit no estado $|0\rangle$ repetidamente absorve e reemite a luz do laser, assim ele fluoresce. Por outro lado, os quBits no estado $|1\rangle$ permanecem escuros.

Devido à sua repulsão mútua de Coulomb, os íons são suficientemente bem separados de modo que eles podem ser individualmente endereçados por pulsos de laser. Se um laser é sintonizado para a freqüência ω da transição e é focado no *n*-ésimo íon, então as oscilações de Rabi[Nielsen e Chuang, 2000] estão induzidas entre $|0\rangle$ e $|1\rangle$. Através da determinação correta do tempo de duração do pulso do laser e pela escolha da fase apropriada para este, os pulsos de laser podem preparar qualquer combinação linear de $|0\rangle$ e $|1\rangle$.

No entanto, a parte mais complicada no projeto e construção de um *hardware* para computação quântica é tomar dois quBits e fazê-los interagir um com o outro. Na armadilha de íons, as interações aparecem devido às repulsões de Coulomb entre os íons. Devido à repulsão mútua, há um espectro de modos normais de vibração para os íons aprisionados pela armadilha. Quando os íons absorvem ou emitem um fóton, o centro de massa do íon recua. Todavia, se o laser é corretamente direcionado, então quando um único íon absorve ou emite um fóton, um

modo normal envolvendo muitos íons irá recuar coerentemente. Isto é conhecido como efeito Mössbauer.

O modo vibracional de freqüência mais baixa, ν, é o modo de centro de massa (cm), em que os íons oscilam em fase, *lockstep* na armadilha. Os íons podem ser resfriados pelo laser para uma temperatura muito menor que ν, assim, cada modo vibracional irá, provavelmente, ocupar seu estado fundamental mecânico-quântico. Agora imagine que o laser seja sintonizado para a freqüência $(\omega - \nu)$ iluminando o *n*-ésimo íon. Para uma duração de pulso propriamente escolhido o estado $|e\rangle_n$ irá transformar-se para $|0\rangle_n$, enquanto o oscilador de centro de massa fará uma transição do estado fundamental $|0\rangle_{cm}$ para seu primeiro estado excitado $|1\rangle_{cm}$, assim um fônon[1] é produzido. Entretanto, o estado $|g\rangle_n|0\rangle_{cm}$ não estará na ressonância para qualquer transição e, deste modo, não estará afetado pelo pulso. Assim, o pulso de laser induz uma transformação unitária atuando como:

$$\begin{aligned} |g\rangle_n|0\rangle_{cm} &\rightarrow |g\rangle_n|0\rangle_{cm}, \\ |e\rangle_n|0\rangle_{cm} &\rightarrow -i|g\rangle_n|1\rangle_{cm} \end{aligned}$$

Esta operação remove um bit de informação que é inicialmente armazenado no estado interno do *n*-ésimo íon, e deposita este bit no estado coletivo de movimento de todos os íons.

Isto significa que o estado de movimento do m-ésimo íon ($m \neq n$) foi influenciado pelo estado interno do *n*-ésimo íon. Neste sentido, houve sucesso na indução de interação entre os íons. Para completar a porta lógica quântica, precisa-se poder transferir a informação quântica do centro de massa de um fônon de volta para o estado interno eletrônico de um dos íons. O processo pode ser implementado já que modo centro de massa sempre retorna seu estado fundamental $\rangle_n|0\rangle_{cm}$ na conclusão da implementação da porta lógica. Por exemplo, Cirac e Zoller[CZ95] mostraram que a porta lógica quântica **XOR**

$$|x, y\rangle \rightarrow |x, y \oplus x\rangle \tag{3.2}$$

pode ser implementada em uma armadilha de íons com um total de 5 pulsos de laser.

Na Tabela 3.1 apresentamos um resumo da implementação de um computador quântico, utilizando-se uma armadilha de íons.

[1] Um fônon é um quantum de energia vibracional

QUADRO-RESUMO

1. Representação do quBit. Estados hiperfinos de um átomo, spins nucleares, e o menor nível vibracional, fônons, de átomos aprisionados nas armadilhas

2. Evolução unitária. Transformações arbitrárias são construídas a partir da aplicação de pulsos de laser que externamente manipulam o estado atômico, numa interação conhecida na literatura como interação de Jaynes-Cummings[Nielsen e Chuang, 2000]. A interação entre os quBits é feita através de estados de fônons compartilhados.

3. Preparação do estado inicial. Resfriar os átomos (por aprisionar e usar extração ótica) dentro de seus estados base de movimento, e estados base hiperfinos.

4. Leitura. Mede-se as populações dos estados hiperfinos.

5. Desvantagens.

a) A duração da vida dos fônons é muito pequena.

b) É muito difícil preparar os íons em seus estados base de movimento.

c) Os computadores quânticos feitos com armadilhas de íons são, por definição, feitos de dispositivos lentos. A velocidade destes dispositivos é limitada, no final das contas, pela incerta relação tempo-energia.

Tabela 3.1: Quadro resumo da implementação de um computador quântico através da utilização de uma armadilha de íons

3.2 Eletrodinâmica quântica cavidade

Um projeto de hardware alternativo (proposto por Pellizari, Gardiner, Cirac e Zoller[CPZ96]) está sendo desenvolvido pelo grupo de Jeff Kimble no Caltech, Instituto de tecnologia da Califórnia[Kimble et al.]. A idéia é aprisionar vários átomos neutros dentro de uma cavidade ótica de altíssima qualidade. A informação quântica pode, então, ser armazenada dentro dos estados internos dos átomos. Contudo, aqui os átomos interagem indiretamente através do seu acoplamento com o modo normal do campo eletromagnético na cavidade (ao invés de modos vibracionais como na armadilha de íons). Novamente, através da sintonização de transições com pulsos de laser, pode-se induzir a transição em um átomo que está condicionada ao estado interno de outro átomo.

Outra possibilidade é armazenar um quBit não no estado interno de um íon, mas na polarização de um fóton. Então, um átomo aprisionado pode ser utilizado como intermediário capaz de fazer com que um fóton interaja com outro fóton (ao invés do fóton ser utilizado para acoplar um átomo a outro).

O grupo de Kimble[Kimble et al.] demonstrou a operação de duas portas lógicas quânticas dois anos atrás. Nesta demonstração, a polarização circular de um fóton influencia a fase de outro fóton.

$$\begin{aligned} |L_1\rangle|L_2\rangle &\rightarrow |L_1\rangle|L_2\rangle \\ |L_1\rangle|R_2\rangle &\rightarrow |L_1\rangle|L_2\rangle \\ |R_1\rangle|L_2\rangle &\rightarrow |L_1\rangle|L_2\rangle \\ |R_1\rangle|R_2\rangle &\rightarrow e^{i\Delta}|R_1\rangle|L_2\rangle \end{aligned} \tag{3.3}$$

onde $|L\rangle$, $|R\rangle$ denotam os estados do fóton com a polarização esquerda (*Left*) e direita (*Right*). Para atingir esta interação, um fóton é armazenado na cavidade, onde o fóton com a polarização $|L\rangle$ não se acopla ao átomo, mas aquele com a polarização $|R\rangle$ o faz fortemente. O segundo fóton, também, interage dando preferência a um átomo de acordo com sua polarização. O pacote de onde do segundo fóton adquire uma fase particular deslocada $e^{i\Delta}$ apenas se ambos os fótons têm polarização $|R\rangle$. Devido ao fato de o deslocamento de fase ser condicionado pelas polarizações de ambos os fótons, esta não é uma porta lógica quântica de dois quBits de fácil construção.

Na Tabela 3.2 apresentamos um resumo da implementação de um computador quântico, utilizando-se eletrodinâmica quâtica de cavidade.

QUADRO-RESUMO
1. *Representação do quBit*. Estado eletrônico de átomos em uma cavidade ótica, ou estado de polarização dos fótons numa cavidade com átomos. 2. *Evolução unitária*. Transformações arbitrárias são construídas a partir de deslocadores de fase (rotações R_z, divisores de luz (rotações R_y), e uma cavidade ótica, para que o campo ótico seja acoplado. 3. *Preparação do estado inicial*. Cria estados de um fóton, através da atenuação da luz laser. 4. *Leitura*. Detecta simples fótons únicos utilizando tubos fotomúltiplicadores. 5. *Desvantagens*. O acoplamento de dois fótons é mediado por um átomo, e deste modo, é desejável aumentar o acoplamento com o campo atômico. Entretanto, acoplar os fótons dentro e fora da cavidade ótica é difícil e limita o cascateamento.

Tabela 3.2: Quadro resumo da implementação de um computador quântico através da utilização da eletrodinâmica quântica de cavidade

3.3 Ressonância magnética nuclear

Um terceiro esquema de hardware, inicialmente desacreditado e que mostrou-se promissor, apareceu há poucos anos e ultrapassou os esquemas de armadilha de íons e cavidade quântica eletrodinâmica para se tornar o mais importante projeto de processamento quântico coerente. Este novo esquema utiliza a tecnologia de ressonância magnética nuclear, RMN. Agora os quBits são os spins nucleares em moléculas particulares. Cada spin pode ser alinhado ($|\uparrow\rangle = |0\rangle$) ou anti-alinhado ($|\downarrow\rangle = |1\rangle$) com um campo magnético aplicado constante. Os spins demoram um longo tempo até relaxar ou tornarem-se decoerentes, assim, os quBits podem ser armazenados por um tempo razoável.

Pode-se também, ligar um campo magnético oscilatório intermitente com freqüência ω (onde ω é a diferença de energia entre os estados *spin-up* e *spin-down*), e induzir as oscilações de Rabi[Nielsen e Chuang, 2000] do spin. Através da determinação adequada do tempo de pulso, pode-se fazer uma transformação unitária desejada sobre um único spin (da mesma forma que discutido nas armadilhas de íons). Todos os spins na molécula são expostos ao campo magnético oscilatório entre si mas apenas aqueles sob ressonância respondem.

Além disso, os spins têm interações dipolo-dipolo, e este emparelhamento pode ser explorado para se fazer uma porta lógica. A diferença de energia entre $|\uparrow\rangle$ e $|\downarrow\rangle$ para um spin depende dos estados dos spins vizinhos.

Tudo isto já era conhecido por químicos há décadas. Apesar disso, foi apenas no ano passado que Gershenfeld e Chuang[GC97] mostraram que a ressonância magnética nuclear providenciava uma implementação útil para computação quântica. Isto não era óbvio por diversas razões. A mais importante é que os sistemas de RMN são muitos quentes. As temperaturas típicas dos spins podem ser da ordem de milhões de vezes maior que a energia entre $|0\rangle$ e $|1\rangle$. Isto significa que os estados quânticos deste computador (os spins em uma mólecula) são muito *ruidosos*— estão sujeitos a intensas flutuações térmicas aleatórias—. Além disso, atualmente, pode-se fazer processamento sobre uma molécula apenas. mas é preciso fazer amostras macroscópicas contendo na ordem de 10^{23} *registradores* e o sinal medido deste dispositivo é a media deste grupo. Os algoritmos quânticos são intrinsicamente probabilísticos, devido à proprio natureza da mecâncica quântica. Por conseguinte, calcular a média sobre o grupo não é equivalente a executar a computação sobre um único dispositivo; o cálculo da média pode obscurecer os resultados.

Gershenfeld e Chuang[GC97] explicaram como superar estas dificuldades. Eles descreveram como *estados efetivos puros* podem ser preparados, manipula-

QUADRO-RESUMO
1. *Representação do quBit*. Spins dos núcleos atômicos. 2. *Evolução unitária*. Tranformações arbitrárias são construídas a partir de pulsos de campos magnéticos aplicados aos spins em um campo magnético forte. Acoplamento entre os spins são providenciados pelos limites químicos entre os átomos vizinhos. 3. *Preparação do estado inicial*. Polarizar os spins por colocá-los em um campo magnético forte, então usar técnicas de preparação de estados efetivos puros. 4. *Leitura*. Medir o sinal de voltagem induzido pelo momento magnético precedente. 5. *Desvantagens*. Esquemas para preparação de estados efetivos puros reduzem o sinal exponencialmente no número de quBits, a menos que a polarização inicial seja suficientemente alta.

Tabela 3.3: Quadro resumo da implementação de um computador quântico através da utilização de RMN

dos e monitorados fazendo-se operações adequadas na temperatura do grupo. A idéia é arranjar as propriedades de flutuação das moléculas para calcular a média quando o sinal for detectado, assim apenas as propriedades coerentes são medidas.

Atualmente já se consegue desenvolver dispositivos de três quBits com esta tecnologia.

Na Tabela 3.3 apresentamos um resumo da implementação de um computador quântico, utilizando-se RMN .

Na Tabela 3.4 apresentamos um teste comparativo das realizações físicas dos computadores quânticos.

Dispositivo	*Principais características*
Fóton	*Podem servir como bons quBits, usando* $\|01\rangle$ *e* $\|10\rangle$ *como 0 e 1 lógicos. Entretanto, materiais óticos não linerares convencionais que sejam suficientemente fortes para permitir interações simples entre os fótons inevitavelmente absorvem ou espalham estes.*
Eletrodinâmica quântica de cavidade	*É uma técnica pela qual átomos únicos podem interagir fortemente com fótons únicos. Isto provê um mecanismo para se usar um átomo para mediarinterações entre fótons.*
Armadilha de íons	*Podem ser congelados de modo a permitir que seus estados nucleares de spin e eletrônicos possam ser controlados através da aplicação de pulsos de laser. Pelo emparelhamento de estados de spin através de fônons de centros de massa, portas lógicas entre diferentes íons podem ser construídas*
Spins nucleares	*Estão muito próximos dos quBits ideais, e moléculas simples poderiam estar próximas de computadores quânticos ideais se seus estados de spin pudessem apenas ser controlados e medidos. A ressonância magnética nuclear torna isto possível usando grandes grupos de moléculas, mas o custo de perda de sinal devido a um ineficiente procedimento de preparação é alto*

Tabela 3.4: Teste comparativo das realizações físicas dos computadores quânticos propostas por [Nielsen e Chuang, 2000]

Capítulo 4

Metodologia

O interesse na Computação Quântica surge devido ao avanço de técnicas de manipulações de sistemas nanoscópicos. Avanço esse que proporcionou que idéias de manipulação quântica de informação pudessem ser implementadas.

Existem atualmente alguns *Processadores Quânticos* implementados, mas eles são muito lentos e possuem pouca memória A computação Quântica é uma das áreas da mais promissoras Ciência, atualmente. Existem vários centros de pesquisa desenvolvendo estudos na área. A Universidade de Oxford, e a de StandFord são alguns dos centros de maior destaque na área.

4.1 Objetivos da pesquisa

O objetivo desse trabalho é dar uma fundamentação teórica ao leitor. É abordada a Física Quântica e seus postulados. O leitor é contextualizado sobre a Computação Quântica. Ficará sabendo de sua história, de suas aplicações, dificuldades de implementação e muitos outros aspectos sobre Processamento Quântico.

4.2 Implementação

O trabalho será realizado em sua grande parte nos laboratórios do Departamento de Ciência da Computação da Universidade Federal de Lavras (UFLA), numa distribuição Red Hat do sistema operacional Linux. A pesquisa será feita pela internet consultando-se sites como:
(`http://www.qubit.org`),
(`http://tph.tuwien.ac.at/~oemer/doc/quprog/`),

(http://www.almaden.ibm.com/st/projects/quantum/intro/),
(http://www.iqi.caltech.edu/),
(http://feynman.media.mit.edu/quanta/nmrqc-darpa/index.html).

Capítulo 5

Evolução temporal e medida de um qubit

5.1 Sistema

Inicialmente o qubit a ser medido é descrito por: $|\psi\rangle = \gamma|+\rangle + \beta|-\rangle$, sendo $\gamma = \frac{1}{\sqrt{2}} + 0i$ e $\beta = 0 - \frac{1}{\sqrt{2}}i$, onde $|+\rangle$ e $|-\rangle$ formam a base ortonormal para esse espaço de estado e são definidas da seguinte maneira: $|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e

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

O campo magnético aplicado é dado por[1]: $\vec{B} = B_x\vec{i} + B_y\vec{j} + B_z\vec{k}$

O momento angular considerado é dado por: $\vec{\sigma} = \sigma_x\vec{i} + \sigma_y\vec{j} + \sigma_z\vec{k}$, onde; $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Estas matrizes são as chamadas matrizes de Pauli.

O hamiltoniano do sistema é dado por: $\vec{H} = \vec{\lambda}.\vec{\sigma}$, onde $\vec{\lambda} = g\ \frac{\hbar}{2}\ \vec{B}$. Nesta equação g é o fator giromagnético, $\hbar$ é a constante de Planck

O operador de evolução temporal é dado por $U(t) = e^{-iHt}$

Para se fazer a medida é necessário seguir os seguintes passos:

(i) encontrar os autovalores de H, resolvendo-se a seguinte expressão: $|H - \alpha\ \mathbf{1}|$, onde $\mathbf{1}$ é o operador identidade

[1] Nas medidas realizadas as componentes B_y e B_z foram condideradas iguais a 0

(ii) Com os autovalores encontrados no item (i), resolve-se $H|\psi\rangle = \alpha|\psi\rangle$ encontrando os coeficientes de $|\psi\rangle$ para cada valor de α.

(iii) Encontrar a expressão do vetor $|\psi\rangle = \gamma|+\rangle + \beta|-\rangle$ em termos dos autovetores de H

Os autovalores de H encontrados no passo (i) são:

$$\begin{aligned} \alpha^2 &= {B_x}^2 + {B_y}^2 + {B_z}^2 \\ \alpha_+ &= +\sqrt{{B_x}^2 + {B_y}^2 + {B_z}^2} \\ \alpha_- &= -\sqrt{{B_x}^2 + {B_y}^2 + {B_z}^2} \end{aligned}$$

No passo (ii) encontramos os seguintes coeficientes para α_+:

$$\begin{aligned} A1 &= A2 * \frac{(B_x - iB_z)}{\alpha_+ - B_z} \\ A2 &= \frac{|\alpha_+ - B_z|}{\sqrt{2 * \alpha^2 - 2 * \alpha_+ * B_z}}, \end{aligned}$$

e para α_-

$$\begin{aligned} B1 &= B2 * \frac{(B_x - iB_z)}{\alpha_- - B_z} \\ B2 &= \frac{|\alpha_- - B_z|}{\sqrt{2 * \alpha^2 - 2 * \alpha_- * B_z}}; \end{aligned}$$

Deste modo os autovetores de H podem ser escritos da seguinte maneira:

$$|\alpha_+\rangle = A1|+\rangle + A2|-\rangle$$

$$|\alpha_-\rangle = B1|+\rangle + B2|-\rangle$$

Etapa (iii):na base $\{|\alpha_+\rangle, |\alpha_-\rangle\}$

$$|\alpha_+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |\alpha_-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ |+\rangle = \begin{pmatrix} A1^* \\ B1^* \end{pmatrix},\ |-\rangle = \begin{pmatrix} A2^* \\ B2^* \end{pmatrix},$$

sendo $A1^*, B1^*, A2^*\ e\ B2^*$ os complexos conjugados de A1, B1, A2 e B2, respectivamente.

O vetor inicial é escrito da seguinte maneira na nova base:
$|\psi\rangle = \gamma|\alpha_+\rangle + \beta|\alpha_-\rangle$

Depois do vetor representado em termos de dos autovetores de H, a expressão que dá a evolução temporal é:

$$U(t)|\alpha\rangle = U(t)|\psi\rangle = e^{-iHt}|\psi\rangle \tag{5.1}$$

A evolução temporal de um sistema quântico de dois níveis, como é o caso do spin do elétron, é a base para o desenvolvimento de qualquer algoritmo quântico.

Foi implementado um programa na linguagem C++ que simula a evolução temporal do Spin de um Elétron em um Campo magnético constante. Este programa é constituído por quatro classes: main.cpp, camMag.h, clmatrix.h, complexo.h. A seguir nós apresentamos uma breve descrição das classes do programa:

main.cpp é a classe principal do programa

camMag.h é utilizada para a criação de um objeto campo magnético

clmatrix.h usada para a se criar objetos do tipo matriz

complexo.h serve para se criar números complexos, que são os índices utilizados na descrição dos estados quânticos

Foram calculadas as probalidades de se encontrar o Spin-Up do Elétron. O campo aplicado tinha somente a componente no eixo X. E o Spin-Up se encontrava na direção do eixo Y. Os resultados obtidos demonstraram que o Spin-Up "realizou" o movimento de precessão em torno do eixo X, o que já era esperado. A Figura 5.1 demonstra tais resultados.

A seguir tomou-se um valor de uma probabilidade em um instante qualquer [2], calculado anteriormente. Com este valor definido realizou-se as seguintes medidas:

- sorteia-se n números aleatórios,
- compara-se os números com o valor da probabilidade,

[2] A probabilidade é diferente em instantes diferentes.

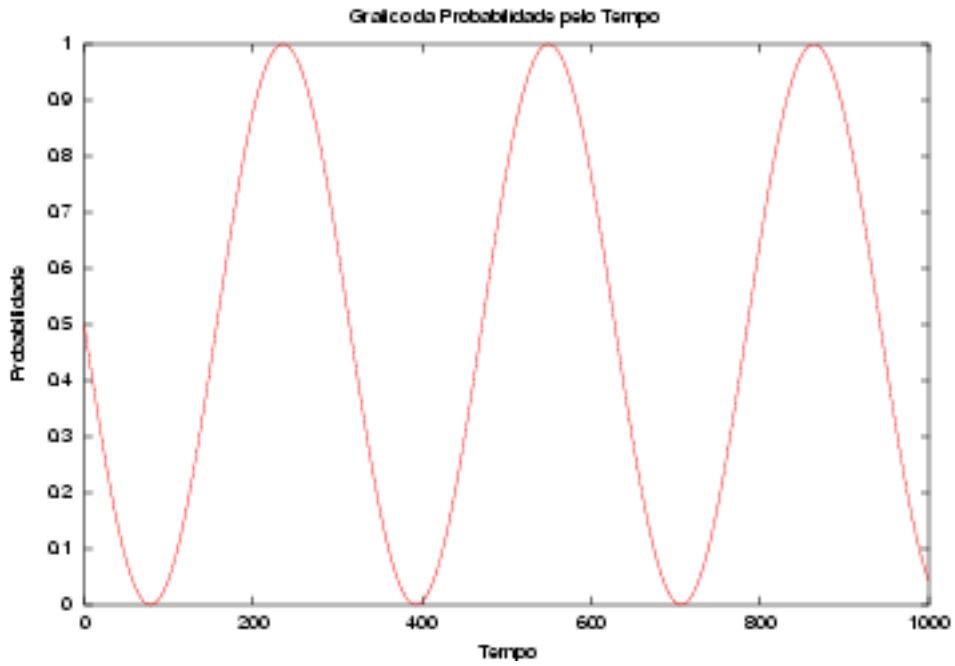

Figura 5.1: Probabilidade

- se o número for menor aumenta-se o contador, que começa com 0,
- depois divide-se o contador por n

Isto é realizado para cada valor de n. Com isto procura-se simular a percentagem de vezes em que se encontra o Spin-Up.

Como o que foi calculado foi a probabilidade de encontrar o Spin-Up, é fácil verificar que quanto maior o número de medidas realizadas, mais o valor se aproxima do provável valor de se obtê-lo. Os resultados das medidas são apresentados nas Figuras 5.2 e 5.3

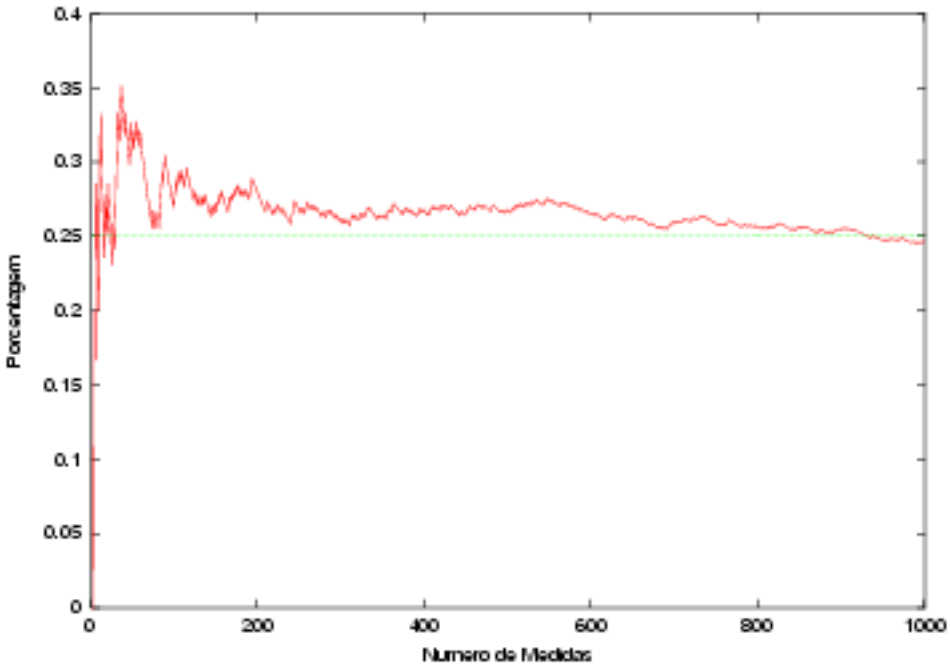

Figura 5.2: Porcentagem entre o número de valores encontrados pelo número de medidas

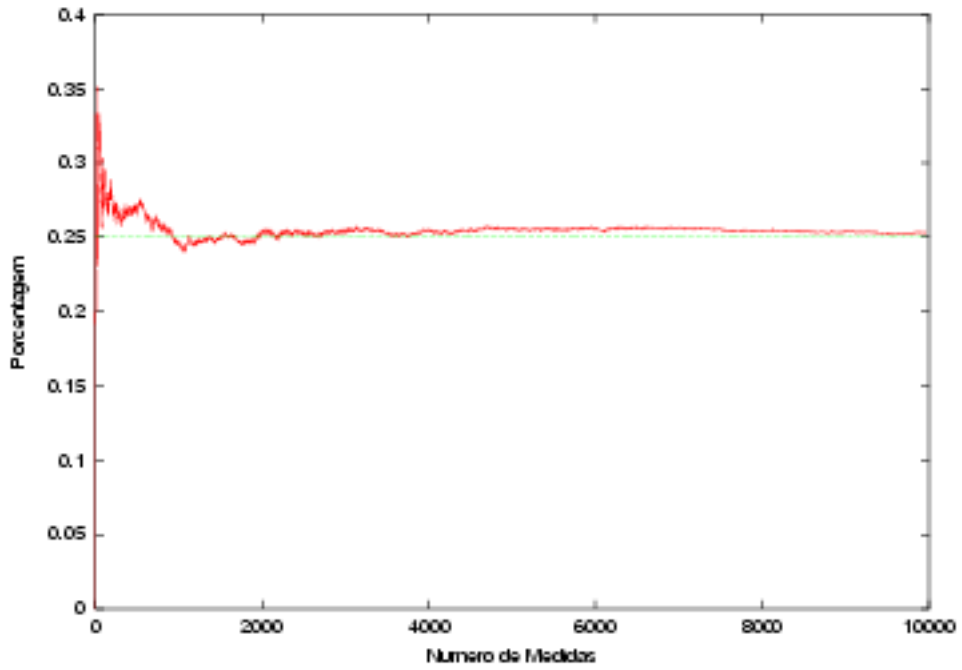

Figura 5.3: Porcentagem entre o número de valores encontrados pelo número de medidas

Capítulo 6

Conclusões

Este capítulo apresenta uma breve conclusão sobre os resultados obtidos com esse trabalho. Foram diversas as dificuldades encontradas. Primeiramente procurou-se entender os Príncípios da Mecânica Quântica, condição básica para o entendimento da Computação Quântica. Depois implementou-se um simulador de evolução temporal do Spin do Elétron num Campo Magnético Uniforme.

6.1 Propostas de trabalhos futuros

O programa implementado é puramente teórico. Os resultados foram obtidos todos através de simulação. O programa pode ter algumas melhorias como:

- criar uma interface gráfica para o programa
- extender para vários elétrons no campo magnético
- considerar o campo magnético variável

6.2 Contribuições

Com este trabalho procurou-se contribruir para a divulgação deste notável campo da computação, que parece ser uma das saídas viáveis para a miniaturização dos componentes elêtronicos. As técnicas de manipulações de sistemas nanoscópicos estão cada vez mais avançadas. Com isto já as pesquisas estão avançando cada vez mais.

6.3 Considerações finais

Cada vez menos gente duvida que os computadores quânticos sejam o futuro da computação. Fatalmente os transístores chegarão ao limite de sua evolução, e para manter a lei de Moore por mais algumas décadas, a única saída seria substituir transístores por átomos.

Num processador quântico, temos átomos ao invés de transístores. Ao invés de bits temos bits quânticos, ou qubits.

Sem dúvida, teríamos gigantescos avanços em praticamente todos os campos, finalmente poderíamos ter códigos de encriptação realmente seguros, pesquisas em gigantescos bancos de dados usando algoritmos inteligentes e traços de inteligência artificial poderiam ser feitas quase instantaneamente, a transmissão de dados poderia alcançar velocidades da ordem de Terabytes por segundo usando fibras ópticas e alta densidade e roteadores quânticos, capazes de lidar com esta quantidade de informação.

A grande pergunta é quando? Ninguém sabe o quão rápido as pesquisas nesta área poderão avançar. Pode demorar cem anos para vermos estas aplicações, ou pode demorar apenas duas ou três décadas. Como é um campo muito novo, não se sabem de onde podem surgir as soluções para os enormes problemas que ainda dificultam a vida dos pesquisadores. Os primeiros computadores quânticos já são realidade, a IBM por exemplo desenvolveu um processador de 5 qubits, que equivalem a um processador de 32 bits, porém operando a meros 200 Hz e precisando de um maquinário gigantesco e caro para funcionar, como os primeiros computadores que tínhamos na década de 40, que acabaram evoluindo até os atuais.

Talvez estejamos, em matéria de tecnologia, em frente à maior descoberta de todos os tempos; talvez, em frente a uma tecnologia de dificílima implementação que pode cair no esquecimento, o fato é que, hoje, essa tecnologia pode ser inegavelmente considerada revolucionária, já que pelas leis da natureza começou a provar-se a possibilidade de solução para problemas de alta complexidade, o que computadores digitais não fariam. Quando entramos no mundo da física quântica e conseqüentemente da computação quântica, temos podido, com certeza; no entanto, encontrar mais problemas do que soluções efetivamente procuradas. Estamos, com certeza, na pré-história da computação quântica, fantasiando supercomputadores, ou mesmo laptops quânticos mas não há como negar que foi dado o primeiro passo, afinal, mostrou-se que existe essa possibilidade.

Referências Bibliográficas

[Deutsch (1985)] Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society of London, 1985, A 400, pp97-117.

[Shor (1994)] Shor, Peter W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings, 35th Annual Symposium on Foundations of Computer Science (IEEE Press, November 1994)

[Jozsa (1997)] Jozsa, Richard. Quantum Algorithms and the Fourier Transform, Submitted to Proc. Roy. Soc. Lond. A for the Proceedings of the Santa Barbara Conference on Quantum Coherence and Decoherence

[Cohen, 1977] Cohen-Tannoudji, Claude at al. Quantum Mechanics, Vol 1. France. Hermann and John Wiley & Sons Inc, 1977.

[Nielsen e Chuang, 2000] NIELSEN, Michel A. e Chuang, Isaac L. Quantum Computation and Quantum Information. Cambridge, UK, Cambridge University Press, 2000.

[Preskill, 2002] PRESKILL, John. Notas de aula do curso de computação quântica. In `http://www.theory.caltech.edu/people/` preskill/ph219

[Kaku, 1998] KAKU, Michio. Visions, How Science Will Revolutionize the 21st Century. New York, September, 1998.

[Lenstra e Lenstra, 1993] LENSTRA, A. e Lenstra, H. The development of the number field sieve. Vol. 1554 of Lecture Notes in Mathematics. Springer Verlag, 1993.

[Rieffel e Polak, 2000] RIEFFEL, Eleanor e Wolfgang. An introduction to quantum computing for non-physicists. In: arXiv:quant-ph/ 9809016 vol. 2. 19 de janeiro de 2000.

[Simon, 1997] SIMON, D. R. On the power of quantum computation. Society for Industrial and Applied Mathematics Journal on Computing 26, 5.

[vonNeumann] John von Neumann, Mathematical Foundations of Quantum Mechanics, Princeton University Press, Princeton, NJ, 1971.

[EPR] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).

[Isham] C.J. Isham, “Lectures on Quantum Theory", Imperial College Press, London, 1997.

[Dirac] P.A.M. Dirac, "Quantum Mechanics", Oxford University Press.

[CZ95] J.I. Cirac and P. Zoller. Quantum computation with cold trapped ions. Phys. Rev. Lett., 74:4091,1995.

[WMI$^+$] D.J. wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *$\mathcal{F}$. Res. Natl. Inst. Stand. Tech.*, 103:259, 1998.

[CPZ96] J.I. Ciraca, T. Pellizzari and P. Zoller. Enforcing coherent evolution in dissipative quantum dynamics. Science, 273:1207, 1996.

[Kimble et al.] J. McKeever, J. R. Buck, A. D. Boozer, A. Kuzmich, H.-C. Naegerl, D. M. Stamper-Kurn, and H. J. Kimble State-Insensitive Cooling and Trapping of Single Atoms in an Optical Cavity, Phys. Rev. Lett. 90, 133602 (2003).

[GC97] N. Gershenfeld and I. L. Chuang. Bulk spin ressonance quantum computation. Science 275:350, 1997

Apêndice A

Suplemento matemático

Neste apêndice apresentamos alguns aspectos mais formais da estrutura matemática da mecânica quântica, que fariam texto principal muito carregado para alguém interessado apenas nos aspectos gerais da computação quântica. Ao invés de deixá-las completamente de fora, resolvemos incluí-las para o benefício do leitor cujo interesse se orienta mais em direção à física e à matemática.

A.1 Operadores

Definimos rapidamente, no Capítulo 2, operadores lineares, sobre um espaço de Hilbert. Vamos apresentar algumas propriedades adicionais desses operadores, importantes para a mecânica quântica. Para maiores detalhes, consultar, por exemplo, [Cohen, 1977] e [vonNeumann].

Um operador linear A agindo sobre um espaço de Hilbert $\mathcal{H}$ é um mapeamento linear que leva um vetor $|f\rangle \in \mathcal{H}$ em um outro vetor $|\phi\rangle = A|f\rangle \in \mathcal{H}$, satisfazendo as seguintes condições:

1. $A(\alpha|f\rangle) = \alpha(A|f\rangle),\ \alpha \in \mathbb{C}$

2. $A(|f\rangle + |g\rangle) = A|f\rangle + A|g\rangle$

Cada operador linear tem um espectro associado, que é o conjunto de soluções da equação de autovalores

$$A|f\rangle = \lambda|f\rangle,\ \lambda \in \mathbb{C}.$$

Este espectro pode ser contínuo ou discreto, dependendo da natureza do operador A. Neste trabalho estaremos interessados em operadores com espectros discretos, ou seja, cujos autovalores podem ser enumerados através de um índice inteiro.

Definimos o produto de dois operadores A e B por

$$(AB)|f\rangle = A(B|f\rangle)$$

Em geral, $AB \neq BA$. Isto significa que a álgebra de operadores lineares em espaços de Hilbert, ao contrário da álgebra de números reais ou complexos, é intrinsecamente não-comutativa. Existem, entretanto, alguns pares de operadores para os quais o produto é comutativo. As relações de comutação entre operadores são tão importantes que definimos a operação

$$[A, B] = AB - BA\,,$$

que chamamos "comutador de A e B". Se $[A, B] = 0$, dizemos que A e B comutam. Uma das consequências de dois operadores A e B comutarem é que um autovetor de A também será autovetor de B. Por isso diz-se que dois observáveis que comutam são *compatíveis*, do ponto de vista de medições.

As relações de comutação entre operadores podem ser usadas para definir operadores. Este é o caso do momento angular. Diz-se que qualquer conjunto de três operadores que satisfazem relações de comutação da forma

$$[L_x, L_y] = iL_z$$

e permutações cíclicas forma um vetor momento angular $\vec{L} = L_x\hat{\imath} + L_y\hat{\jmath} + L_z\hat{k}$

Outro aspecto importante da álgebra de operadores lineares é o que diz respeito a funções de operadores. Uma função f de um operador linear A é um outro operador linear $f(A)$, que definimos por

$$f(A) = \sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!} A^k$$

As considerações sobre a convergência desta série estão fora dos objetivos deste trabalho.

A partir da definição acima, é fácil perceber que, se aplicarmos $f(A)$ a um autovetor $|a_l\rangle$ de A com autovalor a_l, o resultado será

$$f(A)|a_l\rangle = f(a_l)|a_l\rangle\,,$$

desde que a série infinita convirja.

Uma das funções de operadores mais importantes é a exponencial. Ela aparece, por exemplo, na definição do operador de evolução temporal. Como a série de Taylor para a exponencial tem raio de convergência infinito, o operador de evolução temporal está bem definido para qualquer hamiltoniano.

O operador inverso de um operador A, denotado por A^{-1}, também é muito importante. A definição de A^{-1} é

$$A^{-1}A|f\rangle = AA^{-1}|f\rangle = |f\rangle,\ \forall |f\rangle \in \mathcal{H}.$$

A.2 O espaço dual $\mathcal{H}^*$

Quando definimos o produto interno em $\mathcal{H}$, no capítulo 2, introduzimos uma notação especial para representá-lo. Esta notação se baseia na noção de que o produto interno entre dois vetores $|f\rangle, |g\rangle \in \mathcal{H}$, $(|f\rangle, |g\rangle)$ pode ser visto como um *funcional*[1] linear de $|g\rangle$ associado a $|f\rangle$. Denotamos este funcional por $\langle f|$, e dizemos que

$$\langle f|g\rangle \equiv (|f\rangle, |g\rangle)$$

O conjunto dos funcionais lineares associados aos vetores de $\mathcal{H}$ é chamado de espaço dual de $\mathcal{H}$, ou $\mathcal{H}^*$. O fato de que esses funcionais são lineares é consequência de sua definição em termos do produto interno.

Um operador importante pode ser definido com o auxílio do espaço dual. Dizemos que um operador A tem um adjunto (ou hermiteano conjugado) $A^\dagger$ definido da seguinte forma: O vetor de $\mathcal{H}^*$ associado a $A|f\rangle$ é $\langle f|A^\dagger$. Ou seja,

$$(A|f\rangle, |g\rangle) = (|f\rangle, A^\dagger|g\rangle) = \langle f|(A^\dagger|g\rangle) = \langle f|A^\dagger|g\rangle.$$

A.3 Produto tensorial

O espaço de estados de um sistema quântico de uma partícula é um espaço de Hilbert. Se quisermos tratar do problema de várias partículas na mecânica quântica não-relativística, é necessário introduzir o conceito de produto tensorial de espaços de Hilbert. Se duas partículas, quando descritas individualmente, têm seus espaços $\mathcal{H}_A$ e $\mathcal{H}_B$, os estados do sistema conjunto de duas partículas são vetores no espaço de Hilbert $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$. Sejam $\{|1\rangle_A, |2\rangle_A, \cdots, |N\rangle_A\}$ e

[1] Um funcional é uma operação que atribui a um vetor de $\mathcal{H}$ um número $\alpha \in \mathbb{C}$

$\{|1\rangle_B, |2\rangle_B, \cdots, |N\rangle_B\}$ bases dos espaços $\mathcal{H}_A$ e $\mathcal{H}_B$, respectivamente. O conjunto de N^2 elementos $\{|i\rangle_A \otimes |j\rangle_B\}$, $i, j = 1, 2, \cdots, N$ é uma base de $\mathcal{H}_{AB}$. Assim, um vetor $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ pode ser escrito como uma combinação linear dos vetores desta base de $\mathcal{H}_{AB}$:

$$|\psi\rangle \in \mathcal{H}_{AB} \Longrightarrow |\psi\rangle = \sum_{i,j=1}^{N} \alpha_{ij} |i\rangle_A \otimes |j\rangle_B.$$

Ou seja, o espaço de estados das duas partículas tem dimensão N^2 se os espaços das partículas individuais têm dimensão N. A regra para escrever operadores sobre o espaço $\mathcal{H}_{AB}$ é simples: operadores que dizem respeito à partícula A não alteram a parte do produto tensorial relativo à partícula B e vice-versa. Assim, se O_A é um operador que atua em $\mathcal{H}_A$, a extensão deste operador para $\mathcal{H}_{AB}$ é denotada $O_A \otimes 1_B$, onde 1_B é o operador identidade em $\mathcal{H}_B$, e sua atuação sobre os vetores de $\mathcal{H}_{AB}$ é dada por:

$$\begin{aligned}(O_A \otimes 1_B)|\psi\rangle = (O_A \otimes 1_B) \sum_{i,j=1}^{N} \alpha_{ij} |i\rangle_A \otimes |j\rangle_B = \\ \sum_{i,j=1}^{N} \alpha_{ij} (O_A|i\rangle_A) \otimes (1_B|j\rangle_B) = \\ \sum_{i,j=1}^{N} \alpha_{ij} (O_A|i\rangle_A) \otimes |j\rangle_B\end{aligned}$$

A regra para extensões de operadores de $\mathcal{H}_B$ é análoga.

É importante notar que existem estados de $\mathcal{H}_{AB}$ que não podem ser escritos como produto tensorial de estados de $\mathcal{H}_A$ e $\mathcal{H}_B$. Estes são chamados "estados emaranhados", e têm propriedades muito interessantes, tanto que algumas delas são motivo de profundas controvérsias conceituais e filosóficas sobre o status da mecânica quântica como descrição da realidade. O famoso paradoxo de Einstein, Podolsky e Rosen [EPR] pode ser expresso em termos das propriedades aparentemente não locais implicadas pela existência de estados do tipo

$$|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B.$$

Dizer que um sistema quântico composto por dois subsistemas A e B encontra-se num estado deste tipo implica em que existe uma correlação entre os estados das

duas partes que não depende, por exemplo, da separação espacial entre os dois subsistemas. Este tipo de correlação, intrinsecamente quântica, faz com que os dois sistemas se comportem como se um "soubesse" o estado do outro, instantaneamente, mesmo estando os dois infinitamente separados espacialmente. Discutir as consequências conceituais deste tipo de correlação ultrapassa dos objetivos deste trabalho. O leitor interessado poderá consultar a referência [Isham], e artigos variados em revistas de divulgação científica.

Apêndice B

Centros de pesquisa

Atualmente, grande parte parte das pesquisas envolvidas em computação quântica concentra-se no desenvolvimento do hardware. Nesta área, os pesquisadores estão principalmente focados em ressonância magnética.

-IBM's Almaden Research Center: Em agosto de 2000, o físico Isaac Chuang e sua equipe do Centro de Pesquisa de Almaden da IBM anunciaram para o mundo o desenvolvimento do BigBlue. Trata-se de computador quântico de 5 qubits baseados na técnica de rotação do núcleo do átomo (spin up = 1 e spin down = 0) e medição através de ressonância magnética nuclear usada normalmente em hospitais e em laboratórios de química. São cinco átomos de Fluoreno dentro de uma molécula especialmente projetada de forma que os spins do núcleo do fluoreno possam funcionar como qubits programados por radiofrequência. Com esta molécula, a equipe de Chuang resolveu em um único passo um problema matemático para o qual computadores convencionais requereriam repetidos ciclos de execução. O problema, chamado "order-finding"consiste em achar o período de uma determinada função.

Ë um problema matemático típico no qual se baseiam aplicações importantes como a criptografia. Chuang diz que as primeiras aplicações da computação quântica seriam como coprocessadores para funções específicas, tais como busca em uma base de dados e para a solução de difíceis problemas matemáticos.

-Open Qubit - Quantum Computing: Este projeto é desenvolvido por pessoas de todas as partes do mundo. Aqui é feito o compartilhamento de idéias e código sobre a Computação Quântica. O objetivo principal era de escrever um simulador de um computador quântico para demonstrar o algoritmo de fatoração de Shor e sua eficiência na Computação Quântica. Posteriormente, estender este código

para uma API mais genérica que permitiria a implementação de qualquer outro algoritmo quântico.

-National Institute of Standards Technology: Em 1996, seus pesquisadores provaram que pode-se estar ao mesmo tempo em dois lugares separados do espaço (um estado físico da mecânica quântica, denominado superposição).

O experimento publicado no ano de 2000 melhora o trabalho realizado em 1996, no qual os pesquisadores isolaram um íon de Berilium (um átomo sem um de seus elétrons da camada mais externa) em uma armadilha eletromagnética e o resfriaram a uma temperatura perto do zero confinou o íon a uma pequena região do espaço menor que um milionésimo de centímetro, o que ocasiona a sua quase imobilidade.

O que a equipe do NIST fez, diferentemente do ano de 1996 foi separar os dois estados a uma distância de quase 10 átomos. Embora, pareça extremamente pequena para a nossa percepção esta distância é enorme quando tratamos de elétrons. Na verdade o que aconteceu foi que os pesquisadores do NIST cruzaram uma ponte entre a mecânica quântica e o mundo real - o que vemos em nossa vida cotidiana.