Mini-cursos em Matemática Aplicada e Computacional

Editado por

Aarão Lyra
Universidade Potiguar - UnP
Natal, RN, Brasil

Regivan Hugo Nunes Santiago
Departamento de Informática e Matemática Aplicada - DIMAp/UFRN
Natal, RN, Brasil

Sociedade Brasileira de Matemática Aplicada e Computacional

Mini-cursos em Matemática Aplicada e Computacional

1. MC1. Problemas Reais com Modelos em Otimização Combinatória
   Prof. Dr. Elizabeth Gouvêa
2. MC2. Programação Linear Aplicada a Gestão Organizacional
   Prof. Dr. Marco Cesar Goldbarg
3. MC3. Uma Introdução à Computação Quântica
   Prof. Dr. Bernardo Lula Júnior e Aércio Ferreira de Lima
4. MC4. Classificação de Padrões e Clustering
   Prof. Dr. Allan de Medeiros Martins

MC3. Uma Introdução à Computação Quântica

Prof. Dr. Bernardo Lula Júnior
Departamento de Sistemas e Computação
Universidade Federal de Campina Grande
lula@dsc.ufcg.edu.br

Prof. Dr.Aércio Ferreira de Lima
Departamento de Física
Universidade Federal de Campina Grande
aerlima@df.ufcg.edu.br

Sociedade Brasileira de Matemática Aplicada e Computacional

Natal - RN, Brasil
2005

Prefácio

A Computação Quântica é um domínio de pesquisa recente que utiliza elementos de três áreas bem conhecidas: Matemática, Física e Computação. Na visão de um físico (ao menos um dos autores compartilha desta opinião), os conceitos de informação e computação só podem ser corretamente formulados no contexto de uma teoria física: "a informação é armazenada, transmitida e processada sempre por intermédio de um meio físico". Quando efeitos quânticos tornam-se importantes, como, por exemplo, no tratamento de átomos ou fótons individuais, alguns aspectos da lógica clássica que fundamenta a teoria clássica da computação mostram-se curiosamente inadequados. Porém, fenômenos físicos como superposição, interferência e emaranhamento podem ser explorados para tornar possível uma maneira inteiramente nova de tratar a computação e a informação. Neste sentido, é bom lembrar que Computação Quântica não é o mesmo que Física Quântica Computacional ou Química Quântica - assuntos que têm despertado muito interesse atualmente. Não se trata, também, de modelar sistemas quânticos usando computadores clássicos, embora esta seja uma interessante tarefa até mesmo para avaliar o poder da computação atualmente conhecida frente às novas formas propostas. A Computação Quântica trata de "computar"com sistemas quânticos: os chamados computadores quânticos. Esta classe de máquinas oferece, em princípio, a possibilidade de modelar e simular fenômenos quânticos com muito maior eficiência que com os computadores atuais . Problemas até então intratáveis pelas técnicas já conhecidas podem ser resolvidos eficientemente como, por exemplo, o problema da fatoração de grandes números cuja "intratabilidade"fundamenta a criptografia largamente usada na segurança de sistemas de comunicação.

Neste mini-curso pretendemos apresentar os fundamentos da Computação Quântica enfatizando os fenômenos físicos em que ela se baseia. O texto é organizado da seguinte forma: na Introdução apresentamos aspectos importantes da Mecânica Quântica - a teoria física de maior sucesso na explicação dos fenômenos da Natureza; no capítulo dois são apresentadas noções básicas e a notação utilizada para a representação da informação quântica; no capítulo três é feita a descrição do processamento da informação quântica através da utilização do modelo de circuitos quânticos; no capítulo quatro o algoritmo de Deustch é apresentado e analisado segundo o interferômetro de Mach-Zehnder. Por fim, no capítulo cinco, a transformada de Fourier quântica, que é a base da maioria dos algoritmos quânticos importantes, é apresentada e sua utilização é ilustrada para o cálculo do período de uma função.

O texto é apoiado por um software de simulação de circuitos quânticos chamado Zeno, desenvolvido pelo grupo de estudos em computação e informação quântica da Universidade Federal de Campina Grande.

Glossário

Agradecimentos

Conteúdo

Capítulo 1

Introdução: Princípios básicos da Mecânica Quântica

1.1 Dualidade onda-partícula

A Mecânica Quântica é a descrição do comportamento da matéria e da luz em todos os detalhes e em particular do que acontece na escala atômica (ordem de $10^{-10}m$). Os objetos em uma escala tão diminuta comportam-se de maneira distinta de tudo que experimentamos no cotidiano. Na escala atômica os objetos não comportam-se como partículas, nem como nuvens, nem como bolas de bilhar ou com qualquer coisa que tenhamos visto na nossa experiência direta.

A mecânica clássica, por outro lado, trata de fenômenos *macroscópicos* na escala que nos é familiar. Os conceitos clássicos são abstraídos dessa escala de tal forma que podemos formar imagens destes conceitos com base na nossa experiência cotidiana. Não se deve esperar, portanto, que haja acordo entre os conceitos clássicos obtidos de maneira intuitiva pela nossa percepção direta e os fenômenos no mundo atômico e sub-atômico inacessíveis aos nossos sentidos.

Isaac Newton pensava que a luz fosse constituída de partículas, porém, ainda na sua época foi descoberto que ela comportava-se como ondas. Após algum tempo, porém (no começo do século vinte), foi descoberto que a luz às vezes comportava-se como uma partícula. Tal fenômeno, hoje conhecido como efeito fotoelétrico, foi explicado por Albert Einstein em um audacioso trabalho publicado em 1905 sob o título *Um ponto de vista heurístico sobre a produção e a transformação da luz.* A idéia original e audaciosa explorada por Einstein neste trabalho lhe levou a conferir à radiação (luz) uma estrutura discreta e atomística (ou *quantum*). Nascia assim o conceito de fóton, nome que foi dado ao quantum de luz décadas depois (1926).

Fundamentado na nossa percepção e nos nossos sentidos, podemos assegurar que existem dois conceitos da Física Clássica bem definidos cujos atributos, à luz

da nossa experiência diária, nos parece claramente excludentes : onda e partícula.

Uma partícula para a Física Clássica pode ser imaginada como uma bolinha bem pequena que se locomove pelo espaço e que em condições normais não se divide. Além da indivisibilidade, a partícula clássica pode ser considerada possuir uma posição e uma velocidade bem definidas. Com o passar do tempo, a partícula descreve no espaço uma trajetória que é a curva formada pela coleção de posições ocupadas por ela no espaço .

Uma onda, por outro lado, é concebida na Física Clássica como uma excitação que se propaga em um meio, como, por exemplo, uma perturbação em um espelho d'água ocasionada por uma pedra lançada sobre ele. O que se propaga com uma onda é a energia que está associada ao movimento oscilatório das partículas do meio. Como este movimento pode ser tão tênue quanto se queira, diz-se que as ondas não possuem a característica de serem indivisíveis e sim contínuas. Além de serem contínuas e espalhadas no meio, as ondas exibem fenômenos típicos como a *interferência*.

O fenômeno de interferência é de fundamental importância na discussão dos conceitos básicos da Mecânica Quântica. Como discutiremos neste curso, a interferência é também utilizada como ingrediente chave na maioria dos algoritmos quânticos.

1.1.1 Superposição de ondas

Uma onda contínua pode ser representada matematicamente por uma função senoidal (ou cossenoidal). Por exemplo, uma função $\Psi(x,t)$ representando uma onda que se propaga para direita do eixo x é : $\Psi(x,t) = A_0\cos(\frac{2\pi}{\lambda}x - \omega t)$ onde A_0 é a amplitude da onda, λ é chamado comprimento de onda e ω é a freqüência da onda (número de vezes que ela repete seu valor na unidade de tempo). Como uma onda representa um fenômeno que se repete no tempo, dizemos que a onda tem período T se $\Psi(x,t+T) = \Psi(x,t)$. Você pode entender melhor a função $\Psi(x,t)$ fixando uma das variáveis e variando a outra.

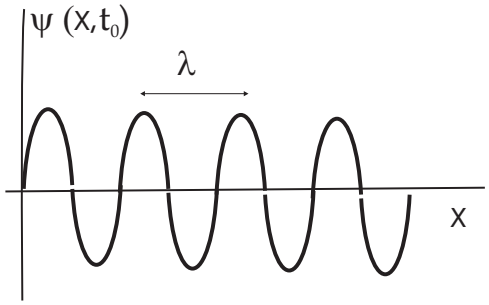

Figura 1.1: Representação de uma onda em uma dimensão

Quando duas ondas se cruzam, como por exemplo, em uma corda, a onda resultante no cruzamento tem uma amplitude que é a soma das amplitudes das ondas

originais. Este é o princípio da superposição da física ondulatória clássica. Quando várias ondas passam por um ponto a amplitude resultante no ponto é a soma das amplitudes das ondas componentes. Para duas ondas contínuas com mesmo comprimento de onda λ propagando-se na mesma direção e sentido, a superposição poderá ser construtiva (ondas em fase) ou destrutiva (ondas deslocadas de $\lambda/2$).

A intensidade de uma onda está relacionada com a energia por unidade de tempo e de área que atravessa um elemento de área perpendicular à direção de propagação da onda. Para nossa onda $\Psi(x,t)$ em uma posição x do espaço num instante t, a intensidade I é dada por

$$I(x,t) = (\Psi(x,t).\Psi^*(x,t)) \propto A(x)^2\cos^2(\omega t + \delta) \tag{1.1}$$

onde δ é uma fase arbitrária [1] .

A luz visível possui freqüência $\omega \sim 10^{15}s^{-1}$ e esta oscilação é tão rápida que o detector registra para a intensidade I em um ponto x do espaço apenas valores médios : $\bar{I} = A(x)^2\langle\cos^2(\omega t + \delta)\rangle = A(x)^2\langle\text{sen}^2(\omega t + \delta)\rangle = 1/2$ (aqui $< ... >$ representa médias temporais tomadas em um ciclo ou período da oscilação).

Exercício 1.1: Mostre que as médias $\langle\cos^2(\omega t - \delta)\rangle$ e $\langle\text{sen}^2(\omega t - \delta)\rangle$ são iguais a 1/2. Use que o valor médio de uma função $f(t)$ num período T é $\langle f(t)\rangle = 1/T\int_0^T f(t)dt$.

Assim sendo, a intensidade é proporcional ao quadrado da amplitude da onda no ponto considerado.

$$\bar{I} = \psi(x)^2 \tag{1.2}$$

onde $\psi(x) = A\cos(\omega t)$.

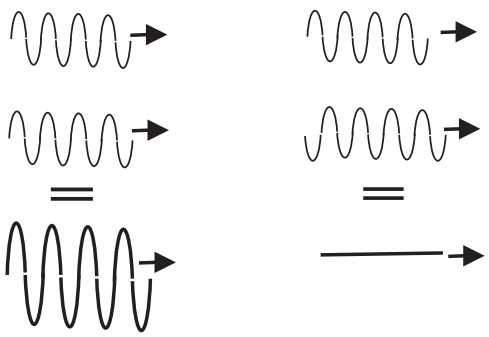

Figura 1.2: Superposição de ondas: à esquerda construtiva(ondas em fase) e à direita destrutiva(ondas fora de fase).

[1] O símbolo $*$ representa o complexo conjugado de um número. Assim, se $z = x + iy$ onde x e y são números reais, $z^* = x - iy$. Então $zz^* = |z|^2 = x^2 + y^2$

Como as ondas se combinam?

A Figura 1.3 mostra uma onda de intensidade I_0 que é dividida em duas partes de igual intensidade I'. Por exemplo, em um espelho semi-prateado (ES)(ver Figura 1.3), qual será a amplitude final de cada onda ? Como $I' = I_0/2$, usando a equação 1.2 concluímos que a amplitude final de cada onda nos caminhos A e B será $\psi' = \psi_0/\sqrt{2}$.

Como será o caminho inverso? Como podemos recombinar os feixes nos caminhos A e B de tal forma que tenhamos a onda original? Veja que se somarmos simplesmente as contribuições das amplitudes das ondas nos caminhos A e B teremos que a amplitude da onda resultante será $\psi_0/\sqrt{2} + \psi_0/\sqrt{2} = \sqrt{2}\psi_0$. Assim, a intensidade final do feixe recombinado será $2I_0$, maior que o feixe inicial! Vê-se portanto que não há maneira simples de conseguir efeito desejado. Existem, porém, regras próprias para se recombinar ondas de forma a conseguir interferência construtiva como veremos na seção 1.2.

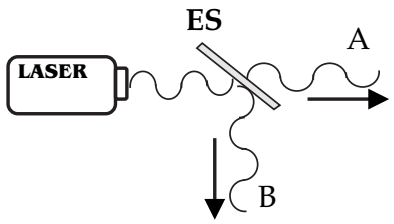

Figura 1.3: Fonte geradora de Laser incidindo um pulso de ondas sobre um espelho semi-prateado ES.

1.2 O Interferômetro de Mach-Zehnder clássico

Vamos apresentar o arranjo experimental envolvendo interferência de ondas conhecido como interferômetro de Mach-Zehnder . Para entender o funcionamento do interferômetro, vamos considerar um feixe de ondas unidimensionais. O primeiro componente do interferômetro é um espelho semi-prateado (ES) que divide a luz em duas partes, uma transmitida e outra refletida de iguais amplitudes. Conforme vimos anteriormente, se a amplitude do feixe inicial for ψ_0, a amplitude do feixe transmitido será $\psi_0/2$, assim como a do feixe refletido.

Além disso, cada componente refletida sofre um deslocamento de fase em relação à transmitida. Usaremos, por convenção, que esse deslocamento de fase é de $\lambda/4$. Isso é válido para espelhos refletores que não absorvem luz.

O esquema do interferômetro de Mach-Zehnder está apresentado na Figura 1.4. O feixe inicial passa pelo espelho semi-prateado $ES1$ e se separa em dois, uma componente transmitida pelo caminho A e outra refletida pelo caminho B. Cada

componente reflete-se nos espelhos E_1 e E_0, e voltam a se cruzar no espelho semi-prateado ES_0, seguindo finalmente para os detectores D_1 e D_0.

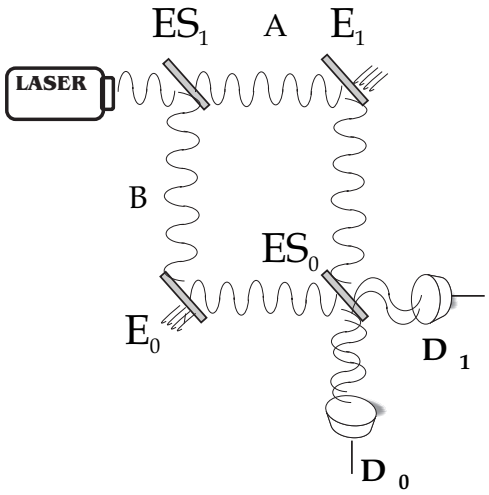

Figura 1.4: Esquema representando o Interferômetro de Mach-Zehnder.

O que acontece nos detectores ?

Como cada componente se divide em duas partes em ES_0, poderíamos esperar que cada detector medisse 50% do feixe. Mas o fato experimental é que 100% do feixe original incide no detector D_1, enquanto o detector D_0 nada registra! O que acontece ?

Explicação: O efeito nos detectores pode ser explicado devido a superposição construtiva dos feixes de onda em D_1 e destrutiva em D_0 (Ver Figura 1.4). O feixe que segue pelo caminho A se aproxima de ES_0 com uma amplitude $\psi_0/\sqrt{2}$ e com um deslocamento de fase relativo de $\lambda/4$ (lembre-se que pela convenção adotada o espelho E_1 introduz esta defasagem); o feixe que segue pelo caminho B aproxima-se de ES_0 com a mesma amplitude porém com uma defasagem de $\lambda/2$, pois sofreu reflexões em ES_1 e E_0. No espelho semi-prateado ES_0, metade do feixe proveniente do caminho A é refletido e metade é transmitido, sendo que a mesma coisa ocorre com o feixe proveniente do caminho B. Consideremos as componentes dos feixes que rumam para o detector D_0. A componente que percorreu o caminho A é transmitida e portanto permanece com a defasagem de $\lambda/4$, passando a ter amplitude $\psi_0/2$ (após divisão do feixe em ES_0). Já o feixe que segue pelo caminho B, é refletido em ES_0 e recebe um acréscimo na defasagem de $\lambda/4$ contabilizando uma defasagem final de $3\lambda/4$ e com amplitude $\psi_0/2$. Temos assim, uma defasagem entre as componentes de mesma amplitude de $\delta = 3\lambda/4 - \lambda/4 = \lambda/2$. Isto resulta numa interferência

destrutiva e, portanto, nada é registrado no detector D_0.

Podemos agora dirimir as dúvidas sobre como acontece a composição dos feixes de onda (como as ondas se combinam ?). Só é possível combinar construtivamente dois feixes de onda que rumam em caminhos diferentes se os dividirmos de tal forma a ocasionarmos uma superposição destrutiva de parte dos componentes resultantes.

1.3 O Interferômetro de Mach-Zehnder quântico

Para transformar o arranjo precedente (Figura 1.4) em um experimento quântico, no qual a dualidade onda-partícula seja relevante, é preciso diminuir a intensidade do feixe até que apenas poucos fótons incidam em ES_1 por vez. Além disso, é preciso utilizar detectores sensíveis à presença de um único fóton. Existem dispositivos conhecidos como fotomultiplicadores que são capazes de produzir um sinal "detectável"em forma de uma corrente elétrica através da absorção de um único fóton . Infelizmente, no estágio atual da tecnologia, a eficiência destes detectores é cerca de 30%. Vale salientar que experimentos ópticos com feixes de fraquíssima intensidade têm sido realizados desde o início do século passado, porém, só a partir de 1985 tornou-se viável a preparação do chamado "estado monofotônico", ou seja, a preparação de um pacote de onda (ou podemos dizer, um feixe de onda) que carrega exatamente um quantum de energia e que atinge o interferômetro num instante bem preciso. Um dos modos de preparar tais feixes é utilizando um processo conhecido como conversão paramétrica onde um único fóton atinge um cristal não-linear (de dihidrogênio fosfato e potássio - KDP) que tem a propriedade de transformar cada fóton incidente em dois, cada um deles com metade da energia do incidente, gerados simultânemente e em direções perfeitamente correlacionadas (em uma dimensão: se um mover-se para esquerda o outro se moveria para direita). Quando um dos fótons do par é detectado em um detector (através de uma fotomultiplicadora, por exemplo) sabe-se com certeza que o outro estará se aproximando de uma porta óptica receptora que se abre no intervalo de tempo preciso deixando o fóton passar. A porta óptica pode ser representada esquematicamente como uma das entradas (ou caminhos) do inteferômetro de Mach-Zehnder quântico, conforme a Figura 1.5, e a representaremos por $|0\rangle$ ou $|1\rangle$. Similarmente ao caso clássico [ver Figura 1.4], na Figura 1.5 podemos ver os espelhos semi-prateados ES_1 e ES_2, os detectores D_0 e D_1 e os espelhos E_1 e E_0. Também podemos ver dois elementos defasadores ϕ_0 e ϕ_1 (estes elementos podem representar por exemplo uma mudança no tamanho do percurso nos braços -caminhos ópticos) do interferômetro responsáveis pela mudança de fase dos feixes de onda.

1.3.1 Análise do interferômetro Mach-Zehnder quântico

O interferômetro de Mach-Zehnder poder ser considerado a versão moderna do experimento de dupla fenda de Young [veja por exemplo a referência ([3]) que descreve em detalhes o experimento], onde as fendas no anteparo são substituídas pelos braços do interferômetro (ver Figura 1.5). Os espelhos semi-prateados (ou

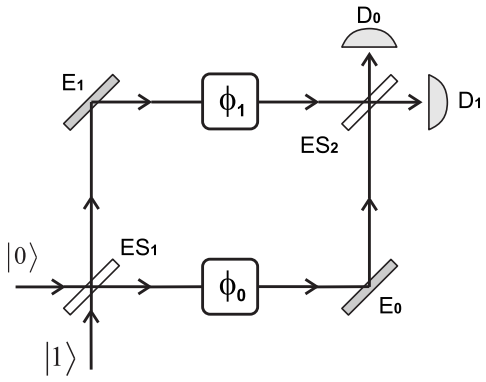

Figura 1.5: Esquema representando o Interferômetro de Mach-Zehnder quântico.

beam splitters), ES_1 e ES_2, refletem ou transmitem o(s) feixe(s) ondulatório(s) nele(s) incidente(s) com taxas de reflexão R e de transmissão T. No caso ideal, ou seja, quando os espelhos não causam perdas no sinal, $R + T = 1$. E_1 e E_0 são espelhos ($R = 1$ e $T = 0$).

A intensidade na saída D_0 pode ser obtida (veja por exemplo [3]) usando os conceitos da Óptica apresentados nas equações (1.3) e (1.4) abaixo:

$$I_{D_0} = \overline{I} \cdot \cos^2\left(\frac{\phi_1 - \phi_2 + k\Delta L}{2}\right) \tag{1.3}$$

$$I_{D_1} = \overline{I} \cdot \text{sen}^2\left(\frac{\phi_1 - \phi_2 + k\Delta L}{2}\right) \tag{1.4}$$

onde $\overline{I}$ é a intensidade média da fonte luminosa, $k = 2\pi/\lambda$ é o número de onda, e ΔL é a diferença no comprimento dos braços do interferômetro.

Sabendo que os possíveis caminhos a serem seguidos pela partícula são $|0\rangle$ ou $|1\rangle$, se uma partícula, por exemplo um fóton, inicialmente no caminho $|0\rangle$, incide em ES_1, terá seu caminho alterado,

$$|0\rangle \longrightarrow i\sqrt{R}\,|1\rangle + \sqrt{T}\,|0\rangle \tag{1.5}$$

ou

$$\begin{aligned} |0\rangle &\longrightarrow i\sqrt{1-T}\,|1\rangle + \sqrt{T}\,|0\rangle \\ |0\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \end{aligned} \tag{1.6}$$

onde consideramos que as taxas de reflexão e transmissão são iguais, $R = 1/2 = T$ e que a reflexão introduz uma fase $e^{i\pi/2} = i$, com relação à transmissão. Observe que isso é consistente com a convenção que adotamos para a defasagem relativa entre

as componentes refletida e a transmitida dos feixes de onda (veja seção 1.2) :

$$\frac{2\pi}{\lambda}x \rightarrow \frac{2\pi}{\lambda}\left(x+\frac{\lambda}{4}\right) = \frac{2\pi}{\lambda}x + \frac{\pi}{2}$$

Se, por outro lado, a partícula, antes de incidir em ES_1, estivesse no caminho $|1\rangle$:

$$\begin{aligned} |1\rangle &\longrightarrow i\sqrt{1-T}\,|0\rangle + \sqrt{T}\,|1\rangle \\ |1\rangle &\longrightarrow \frac{1}{\sqrt{2}}\,i(|0\rangle - i|1\rangle) \end{aligned} \tag{1.7}$$

Note que o que distingue os estados (1.6) e (1.7) é a fase relativa $e^{i\pi} = -1$ entre os caminhos $|0\rangle$ e $|1\rangle$ constituintes. Assim, podemos descrever o efeito dos dispositivos $ES_{1(2)}$ como produzindo uma superposição de estados distintos e uma fase relativa entre eles.

A operação efetuada pelos espelhos semi-prateados ES (com $R = T = 1/2$) sobre os caminhos $|0\rangle$ e $|1\rangle$, pode ser representada, como ficará claro no próximo capítulo, pela operação unitária U_{ES}

$$U_{ES} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{1.8}$$

Com objetivo de prosseguir com nossa análise do interferômetro de Mach-Zehnder quântico (antecipando-se a notação que será utilizada no próximo capítulo), podemos, como justificativa provisória, identificar os rótulos dos caminhos do interferômetro, $|0\rangle$ e $|1\rangle$, com as direções no espaço bi-dimensional:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{e} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Não é difícil verificar que (1.8) satisfaz (1.6-1.7),

$$\begin{aligned} U_{ES}\,|0\rangle &= \frac{1}{\sqrt{2}}\,(|0\rangle + i|1\rangle) \\ U_{ES}\,|1\rangle &= \frac{i}{\sqrt{2}}\,(|0\rangle - i|1\rangle) \end{aligned} \tag{1.9}$$

Os espelhos E_1 e E_2 não alteram significativamente os resultados relativos (1.6-1.7). O efeito dos espelhos pode ser representado pela operação U_E

$$U_E = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.10}$$

Mais explicitamente,

$$\begin{aligned} U_E|0\rangle &= |1\rangle \\ U_E|1\rangle &= |0\rangle \end{aligned} \tag{1.11}$$

O caminho seguido pela partícula no interferômetro a partir do seu estado inicial $|0\rangle$ (veja Figura 1.5) pode agora ser representado por

$$\begin{aligned} |0\rangle \quad & \xrightarrow{ES_1} \quad \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \\ & \xrightarrow{\phi_0, E_0, \phi_1, E_1} \quad \frac{1}{\sqrt{2}}(e^{i\phi_0}|1\rangle + ie^{i\phi_1}|0\rangle) \\ & \longrightarrow \quad ie^{i(\phi_1+\phi_0)/2}\frac{1}{\sqrt{2}}[e^{i(\phi_0-\phi_1)/2}|1\rangle + \\ & \qquad ie^{-i(\phi_0-\phi_1)/2}|0\rangle] \\ & \xrightarrow{ES_2} \quad ie^{i\frac{\phi_0+\phi_1}{2}} \\ & \qquad [\cos\frac{(\phi_0-\phi_1)}{2}|0\rangle + \\ & \qquad \operatorname{sen}\frac{(\phi_0-\phi_1)}{2}|1\rangle] \equiv |\Psi_{ES2}\rangle \end{aligned} \tag{1.12}$$

Os detectores D_0 e D_1 registram a presença da partícula em cada uma das possíveis saídas.

A detecção é feita em D_0 ou D_1 através da medição da intensidade da onda associada à partícula, que como vimos, é proporcional ao quadrado do módulo da amplitude da mesma. Assim, a intensidade registrada no detector D_0, para uma partícula vinda inicialmente pelo caminho "$|0\rangle$", é definida por

$$I_0^{|0\rangle} = \cos^2\frac{(\phi_0-\phi_1)}{2} \tag{1.13}$$

E para o detector D_1, encontra-se

$$I_1^{|0\rangle} = \operatorname{sen}^2\frac{(\phi_0-\phi_1)}{2} \tag{1.14}$$

Se o caminho inicial da partícula fosse "$|1\rangle$" teríamos as intensidades medidas nos detectores D_0 e D_1 dadas por

$$I_0^{|1\rangle} = \operatorname{sen}^2\frac{(\phi_0-\phi_1)}{2} \tag{1.15}$$

e

$$I_1^{|1\rangle} = \cos^2\frac{(\phi_0-\phi_1)}{2} \tag{1.16}$$

Observe que podemos recuperar o resultado obtido na discussão do interferômetro clássico [ver secção 1.2]. Basta considerar a defasagem $\delta = \phi_0 - \phi_1 = 0$ nas equações

1.13 e 1.14. Note que surpreendentemente chegamos à conclusão que mesmo para um único fóton incidindo numa das "portas"do interferômetro, ele deve interagir consigo mesmo de tal forma a produzir interferência construtiva num dos detectores e destrutiva no outro, à semelhança do que foi discutido na seção 1.2.

Capítulo 2

Representação da informação

2.1 O qubit

A unidade básica de informação nos computadores clássicos é o *bit* (*binary digit*), que pode ser (ou tem valor) 0 ou 1. Então, para representar uma informação, codificada numa sequência finita de bits, um computador deve conter uma coleção correspondente de sistemas físicos, cada um dos quais deve existir (ou pode estar) em dois estados físicos distingüíveis e não ambíguos associados aos valores (0 ou 1) do bit que o sistema físico representa . Um exemplo de um sistema físico capaz de representar um bit é o de uma chave mecânica (ou eletrônica) de duas posições (estados) que implementa uma "barreira de energia"entre os estados para impedir transições espontâneas.

Em um computador quântico, um sistema quântico de 2 estados é utilizado para representar um bit, sendo então chamado de *quantum bit* (ou *qubit*). No entanto, além da possibilidade de existir (ou de estar) em um dos dois estados que representam os valores 0 ou 1 (e que são chamados de $|0\rangle$ ou de $|1\rangle$, respectivamente), um qubit tem a peculiaridade de existir (ou de estar) em uma mistura desses dois estados simultaneamente, o que é conhecido como uma *superposição coerente de estados*. Em termos matemáticos, o estado geral de um qubit (denotado usualmente por $|\psi\rangle$) é descrito por um vetor unitário em um espaço de Hilbert bidimensional ($\mathbb{C}^2$):

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{2.1}$$

Com as amplitudes α_0 e $\alpha_1 \in \mathbb{C}$ e satisfazendo $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Os dois estados clássicos possíveis, denotados pelos *kets* $|0\rangle$ e $|1\rangle$, formam uma base para este espaço chamada de *base computacional*. Os kets $|0\rangle$ e $|1\rangle$ representam os vetores:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad e \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

e, então, $|\psi\rangle \equiv \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$

Ao contrário de um bit no caso clássico, que tem um valor determinado em qualquer tempo, o valor de um qubit no estado $|\psi\rangle$ é indeterminado. De acordo com a Física Quântica, uma medição de $|\psi\rangle$ na base computacional daria como resultado o valor 0 em $|\alpha_0|\%$ das vezes e o valor 1 nas outras $|\alpha_1\%|$ das vezes. O processo de medição altera o estado do sistema (qubit) fazendo-o assumir o estado $|0\rangle$, com probabilidade $|\alpha_0|^2$, ou o estado $|1\rangle$, com probabilidade $|\alpha_1|^2$ (o que explica a restrição $|\alpha_0|^2 + |\alpha_1|^2 = 1$ acima). Os valores de α_0 e α_1 não podem ser conhecidos através de uma medição, que é a "interface"entre o nível clássico e o nível quântico e a única maneira de acesso à informação contida no nível quântico.

Existe uma interpretação geométrica para um qubit em $\mathbb{R}^3$ e que ajuda no entendimento das propriedades de um qubit. Como $|\alpha_0|^2 + |\alpha_1|^2 = 1$, a equação 2.1 pode ser reescrita como :

$$|\psi\rangle = e^{i\gamma}\left(\cos(\theta/2)|0\rangle + e^{i\phi}\text{sen}(\theta/2)|1\rangle\right), \tag{2.2}$$

onde θ, ϕ e $\gamma \in \mathbb{R}$. Como o termo $e^{\imath\gamma}$ (chamado *fator de fase global*) não tem efeito físico observável (lembre que $|e^{i\gamma}| = 1$), pode ser desconsiderado e a equação (2.2) se transforma em :

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\text{sen}(\theta/2)|1\rangle \tag{2.3}$$

Os números $\theta \in [0, \pi]$ e $\phi \in [0, 2\pi]$, definem um ponto na esfera tridimensional de raio igual 1 (chamada *esfera de Bloch*), como mostrado na figura abaixo :

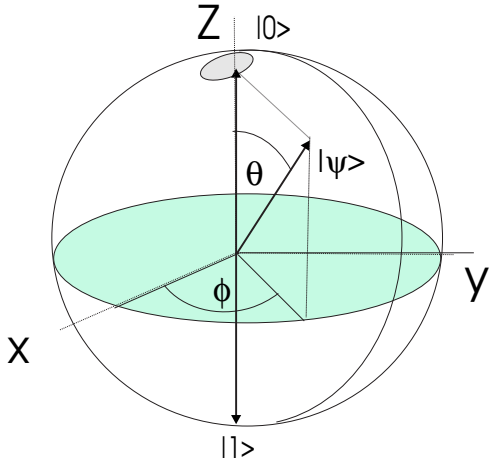

Figura 2.1: Esfera de Bloch

O ângulo θ que o vetor faz com o eixo vertical (eixo Z) está relacionado com as "contribuições "relativas dos estados da base $|0\rangle$ e $|1\rangle$ para o estado geral do qubit. O ângulo ϕ que a projeção do vetor sobre o plano $x - y$ faz com o eixo x

corresponde à fase relativa do qubit. O fator de fase relativa embora não altere as contribuições relativa do qubit nos estados da base, tem importância capital nos efeitos de interferência utilizados pelos algoritmos quânticos. Assim, um estado pode ter as mesmas proporções de $|0\rangle$'s e $|1\rangle$'s mas ter diferentes amplitudes devido a fatores de fase relativa diferentes.

Exercício 2.1: Mostre que a representação polar no $\mathbb{R}^3$ de um estado qualquer é dada por : $(x, y, z) = (\cos\phi\text{sen}\theta, \text{sen}\phi\text{sen}\theta, \cos\theta)$, com $0 \leq \theta \leq \pi$ e $0 \leq \phi \leq 2\pi$.

2.2 Espaço de Hilbert e produtos interno e exterior

Um espaço de Hilbert n-dimensional $\mathcal{H}$ é um espaço vetorial complexo de dimensão n equipado com produto interno. Os espaços $\mathbb{C}^n$ (n inteiro, finito e maior que 1), são exemplos de espaços de Hilbert[1]. A existência de produto interno dota o espaço de uma noção natural de distância. O *produto interno* de dois vetores $|\phi\rangle$ e $|\psi\rangle \in \mathbb{C}^n$, denotado por $\langle\phi|\psi\rangle$, é definido como o produto matricial entre $|\phi\rangle^\dagger$ e $|\psi\rangle$, ou seja, o número complexo dado por:

$$\langle\phi|\psi\rangle \;=\; (|\phi\rangle)^\dagger|\psi\rangle \;=\; \sum_{i=1}^{n} \phi_i^* \psi_i \tag{2.4}$$

O vetor $|\phi\rangle^\dagger$ é chamado vetor *dual* de $|\phi\rangle$, denotado por $\langle\phi|$, e ϕ_i^* é o conjugado complexo da i-ésima componente ϕ_i do vetor $|\phi\rangle$.

O produto interno satisfaz as seguintes regras:

1. $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$,
2. $\langle\phi|(a|u\rangle + b|v\rangle) = a\langle\phi|u\rangle + b\langle\phi|v\rangle$,
3. $\langle\phi|\phi\rangle \geq 0$
4. $\langle\phi|\phi\rangle = 0 \Leftrightarrow |\phi\rangle = \mathbf{0}$

com $a, b \in \mathbb{C}$ e $|\phi\rangle$, $|\psi\rangle$, $|u\rangle$ e $|v\rangle \in \mathbb{C}^n$

A *norma* de um vetor $|\psi\rangle$, denotada por $|||\psi\rangle||$, é definida por $|||\psi\rangle|| = \sqrt{\langle\psi|\psi\rangle}$ e dois vetores são *ortogonais* se seu produto interno é zero,ou seja, $\langle\phi|\psi\rangle = 0$.

O produto *exterior* entre dois vetores $|\phi\rangle \in \mathbb{C}^m$ e $|\psi\rangle \in \mathbb{C}^n$, denotado por $|\phi\rangle\langle\psi|$, é uma matriz $m \times n$ dada por $|\phi\rangle(|\psi\rangle)^\dagger$. Dada uma base $\{|i\rangle\}$ para um espaço de Hilbert n-dimensional, o produto exterior tem a seguinte propriedade (completude): $\sum_{i=1}^{n} |i\rangle\langle i| = \mathbf{I}$.

Exercício 2.2 : Mostre que o conjunto $\{|0\rangle, |1\rangle\}$ forma uma base ortonormal para $\mathbb{C}^2$

[1]Há outras definições matematicamente mais rigorosas que permitem tratar espaços de dimensão infinita. Para os nossos propósitos a definição aqui utilizada será suficiente

Exercício 2.3: Mostre que para quaisquer dois vetores $|\phi\rangle$ e $|\psi\rangle \in \mathbb{C}^n$, $(|\psi\rangle\langle\psi|)|\phi\rangle = \langle\psi|\phi\rangle|\psi\rangle$

2.3 Estado geral de um registrador de memória quântico

Até então, descrevemos o estado de um sistema quântico simples de dois estados, ou seja, o estado de um qubit. Porém, assim como em um computador clássico, um *registrador de memória* em um computador quântico deve consistir de uma coleção de qubits. Então, como devemos descrever seu estado ?

A Física Quântica descreve o estado genérico de um sistema composto de n qubits ($|\psi\rangle$) como uma superposição normalizada dos 2^n estados da base computacional $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$ do espaço $\mathbb{C}^{2^n}$, ou seja,

$$|\psi\rangle \;=\; \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \qquad \text{com a restrição} \sum_{x=0}^{2^n-1} |\alpha_x|^2 \;=\; 1 \tag{2.5}$$

Assim, o estado geral $|\psi\rangle$ de um sistema com n qubits é descrito por um vetor unitário no espaço $\mathbb{C}^{2^n}$ com amplitudes α_i, $0 \leq i \leq 2^n$.

Por exemplo, o estado geral de um sistema de dois qubits é uma superposição dos estados da base computacional $|0\rangle, |1\rangle, |2\rangle$ e $|3\rangle$, ou, na notação binária $|00\rangle, |01\rangle, |10\rangle$ e $|11\rangle$:

$$|\psi\rangle \;=\; \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{2.6}$$

com a restrição

$$\sum_{i,j=0}^{1} |\alpha_{ij}|^2 = 1. \tag{2.7}$$

Um tipo especial de estado é o chamado *produto direto* que é descrito pelo produto tensorial dos estados de seus componentes. Por exemplo, se $|\psi\rangle_A$ e $|\phi_B\rangle$ são os vetores de estado de dois qubits A e B nos espaços de Hilbert $\mathcal{H}_A$ e $\mathcal{H}_B$, $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$:

$$|\psi\rangle_A = \left[\begin{array}{c} \psi_0 \\ \psi_1 \end{array}\right]_A \qquad \text{e} \quad |\phi\rangle_B = \left[\begin{array}{c} \phi_0 \\ \phi_1 \end{array}\right]_B$$

ou de outra forma,

$$|\psi\rangle_A \;=\; \psi_0|0\rangle_A + \psi_1|1\rangle_A \qquad \text{e} \qquad |\phi\rangle_B = \phi_0|0\rangle_B + \phi_B|1\rangle_B,$$

então, o estado produto direto do sistema composto pelos dois qubits, $|\psi\rangle_{AB}$, é obtido pelo produto tensorial de $|\psi\rangle_A$ com $|\phi\rangle_B$:

$$|\psi\rangle_{AB} \;=\; |\psi\rangle_B \otimes |\phi\rangle_B \;=\; \left[\begin{array}{c} \psi_0\phi_0 \\ \psi_0\phi_1 \\ \psi_1\phi_0 \\ \psi_1\phi_1 \end{array}\right]_{AB} \tag{2.8}$$

O vetor resultante $|\psi\rangle_{AB}$ é um vetor no espaço $\mathbb{C}^{2^2} = \mathbb{C}^2 \otimes \mathbb{C}^2$ gerado pela base :

$$\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}.$$

onde $\{|0\rangle_A, |1\rangle_A\}$ e $\{|0\rangle_B, |1\rangle_B\}$ são as bases computacionais dos espaços associados aos qubits A e B, respectivamente, ou seja :

$$\begin{aligned}
|\psi\rangle_A \otimes |\phi\rangle_B &= \left(\psi_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \psi_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)_A \otimes \left(\phi_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \phi_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)_B = \begin{bmatrix} \psi_0 \\ \psi_1 \end{bmatrix}_A \otimes \begin{bmatrix} \phi_0 \\ \phi_1 \end{bmatrix}_B \\
&= \begin{bmatrix} \psi_0\phi_0 \\ \psi_0\phi_1 \\ \psi_1\phi_0 \\ \psi_1\phi_1 \end{bmatrix}_{AB} \\
&= (\psi_0|0\rangle_A + \psi_1|1\rangle_A) \otimes (\phi_0|0\rangle_B + \phi_1|1\rangle_B) \\
&= \psi_0\phi_0|0\rangle_A \otimes |0\rangle_B + \psi_0\phi_1|0\rangle_A \otimes |1\rangle_B + \psi_1\phi_0|1\rangle_A \otimes |0\rangle_B + \psi_1\phi_1|1\rangle_A \otimes |1\rangle_B \quad (2.9)
\end{aligned}$$

que podemos simplificar omitindo o símbolo $\otimes$

$$\begin{aligned}
|\psi\rangle_A \otimes |\phi\rangle_B &= \psi_0\phi_0|0\rangle_A|0\rangle_B + \psi_0\phi_1|0\rangle_A|1\rangle_B + \psi_1\phi_0|1\rangle_A|0\rangle_B + \psi_1\phi_1|1\rangle_A|1\rangle_B \\
&= \sum_{i,j=0}^{1} \psi_i\phi_j|i\rangle_A|j\rangle_B \quad (2.10)
\end{aligned}$$

Podemos simplificar ainda mais a notação, omitindo a indicação do espaço e escrevendo $|00\rangle$ em lugar $|0\rangle|0\rangle$, $|01\rangle$ em lugar de $|0\rangle|1\rangle$, etc, obtendo:

$$\begin{aligned}
|\psi\rangle_A \otimes |\phi\rangle_B &= \sum_{i,j=0}^{1} \psi_i\phi_j|ij\rangle \\
&= \psi_0\phi_0|00\rangle + \psi_0\phi_1|01\rangle + \psi_1\phi_0|10\rangle + \psi_1\phi_1|11\rangle \quad (2.11)
\end{aligned}$$

Note que o estado geral de dois qubits (2.6) é da forma produto direto (2.11) se e somente se,

$$\alpha_{00} = \psi_0\phi_0\,,\ \alpha_{01} = \psi_0\phi_1,\ \alpha_{10} = \psi_1\phi_0\,,\ \alpha_{11} = \psi_1\phi_1$$

ou seja, $\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$. Visto que as amplitudes em (2.6) são regidas apenas pela condição de normalização (2.7), essa relação não é geral, e portanto, o estado geral de dois qubits nem sempre é o produto direto dos estados dos qubits individuais. Por exemplo, o estado $(|00\rangle + |11\rangle)/\sqrt{2}$ não pode ser escrito como um estado produto direto de estados de um qubit. Quando isto ocorre, o estado é dito ser ou estar *emaranhado*.

Uma medição do estado genérico $|\psi\rangle$ de n qubits produz um resultado x, $0 \leq x \leq 2^n - 1$, e o estado após a medição será $|x\rangle$. Usualmente, a medição é realizada qubit a qubit, produzindo zeros e uns que são lidos em conjunto como um número binário

de n bits. O procedimento de medição altera inevitavelmente $|\psi\rangle$, forçando-o a um "colapso"para algum estado da base computacional com probabilidades dadas pelos quadrados dos módulos das amplitudes de $|\psi\rangle$.

Uma propriedade interessante e utilizada em muitos algoritmos quânticos é que se o estado de registrador quântico está emaranhado, então, os valores que podem ser obtidos pela medição de qubits na seqüência serão determinados pelos resultados das medições realizadas nos qubits anteriores. Essa propriedade nos permite alterar o estado de uma parte do registrador simplesmente medindo outra parte do registrador.

Além disso, a expressão (2.5) que descreve o estado de um *registrador quântico* de n qubits, nos permite inferir que, diferentemente de um registrador clássico de n bits que pode ser preparado apenas em um dos 2^n estados possíveis, um registrador quântico de n qubits pode ser preparado num superposição de todos os 2^n estados possíveis, o que abre a possibilidade de processamento simultâneo de todas as entradas possíveis com apenas uma aplicação do procedimento em vista, o que é chamado *paralelismo quântico* .

Capítulo 3

Processamento da Informação

3.1 O computador clássico

Em um computador clássico, o processamento da informação codificada em bits é realizado por dispositivos chamados *circuitos lógicos*. Uma máquina clássica pode ser vista como um dispositivo que converte univocamente uma seqüência de bits (entrada) em outra seqüência de bits (saída), ou seja, a cada seqüência de n bits de entrada, faz corresponder um único conjunto de n bits de saída, o que caracteriza sua ação como o cálculo de uma função $f : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$, onde $N = 2^n$ e n é o número de bits dos registradores de memória. As funções f passíveis de serem calculadas (ou computadas) por tais dispositivos formam a classe das *funções computáveis* e que podem ser descritas a partir de funções booleanas elementares AND,OR e NOT. No modelo de circuitos lógicos (ou digitais), o processo de cálculo (o algoritmo) de f é descrito por um circuito formado por blocos elementares chamados *portas lógicas*, que podem ser fisicamente realizadas por transistores e outros componentes eletrônicos, e que implementam as funções booleanas elementares. Representando as portas NOT e AND, como na Figura 3.1 e conectando as portas umas às outras por fios, podemos representar um circuito

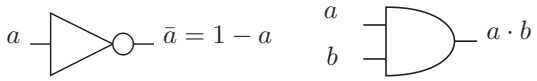

Figura 3.1: Portas NOT e AND, respectivamente. A ação da porta NOT é negar o bit de entrada a e a ação da porta AND é multiplicar os bits a e b da entrada.

lógico através de um diagrama. Por exemplo, o diagrama da Figura 3.2 representa um circuito lógico que realiza (ou computa) a função $f(x, y) = x \oplus y$, onde $\oplus$ é

operador de adição módulo 2.

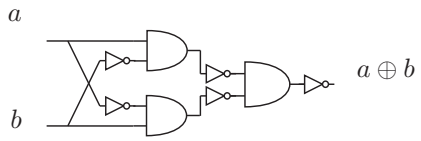

Figura 3.2: Circuito que computa a função adição módulo 2.

O circuito da Figura 3.2 é *irreversível*, isto é, não é possível obter de volta os valores dos bits de entrada a partir do valor do bit de saída. As portas elementares AND e OR são irreversíveis. No entanto é possível transformar um circuito lógico qualquer irreversível em um circuito lógico reversível. Para tanto, podemos usar a porta Toffoli que implementa todas as portas lógicas elementares de forma reversível, de acordo com a Figura 3.3:

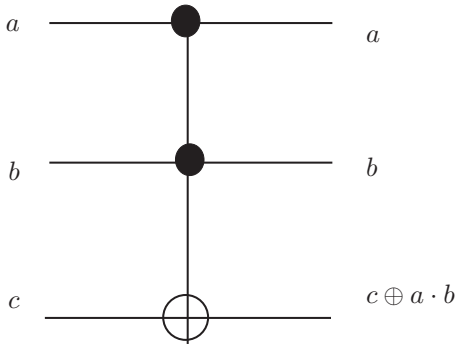

Figura 3.3: Porta Toffoli

$$c \oplus a \cdot b \quad = \quad \begin{cases} a \cdot b \quad \text{para} \quad c = 0 \quad (AND) \\ a \oplus c \ \text{para} \quad b = 1 \quad (XOR) \\ \bar{c} \quad \text{para} \quad a = b = 1 \quad (NOT) \\ \overline{a \cdot b} \quad \text{para} \quad c = 1 \quad (NAND) \\ a \quad \text{para} \quad b = 1, c = 0 \quad (FANOUT) \end{cases} \tag{3.1}$$

Exercício 3.1: Mostre que a porta Toffoli é reversível.

A eficiência com que um computador calcula uma função f pode ser comparada com o número de portas usadas no circuito que calcula f. Se o número de portas no circuito cresce polinomialmente com o tamanho da entrada (o número de bits n), dizemos que o circuito é *eficiente*. Se, por outro lado, o número de portas no circuito cresce exponencialmente com n, dizemos que o circuito é *ineficiente*.

3.2 O computador quântico

3.2.1 Operação unitária

A teoria quântica nos diz que a evolução no tempo de um sistema quântico isolado é descrita matematicamente por uma transformação linear. Como os vetores de estados quânticos são unitários (módulo igual a um), uma transformação linear U que preserva o módulo dos vetores é uma *transformação unitária*, isto é, atende a seguinte propriedade

$$U^\dagger U = UU^\dagger = I \tag{3.2}$$

onde $U^\dagger = (U^*)^T$, ou seja, a conjugada transposta de U.

Então, uma conseqüência imediata da definição do processo evolutivo de um sistema quântico como um processo unitário (descrito por uma operação unitária) é que ele é reversível. Usaremos no texto que segue os termos operação e operador linear para fazer referência tanto à transformação linear quanto à matriz que a representa.

A linguagem mais usada atualmente na descrição do processamento quântico da informação é a linguagem dos *circuitos quânticos*, similar à linguagem dos circuitos lógicos clássicos : circuitos quânticos são agrupamentos ou malhas de dispositivos mais simples chamados portas quânticas que realizam em conjunto uma operação unitária sobre um registrador quântico. Uma porta especial de medição permite a observação ou medição do estado de um qubit.

3.2.2 Portas quânticas de 1-qubit

Uma porta quântica simples (porta de 1-qubit) realiza uma operação unitária U (representada por uma matriz 2×2) sobre o estado $|\psi\rangle$ de um qubit fazendo-o evoluir para o estado $U|\psi\rangle$. Enquanto no caso clássico temos apenas uma porta lógica que pode atuar sobre um bit, a porta lógica NOT, no caso quântico temos um número infinito de portas quânticas simples (conjunto de matrizes unitárias 2×2). A seguir, apresentamos as portas quânticas elementares de 1-qubit .

A porta quântica X tem o mesmo efeito da porta lógica NOT quando aplicada aos estados da base computacional de um qubit, ou seja, $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$, e tem a seguinte expressão matricial

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3.3}$$

Porém, se o estado do qubit for uma superposição dos estados $|0\rangle$ e $|1\rangle$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, o estado resultante será $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$. O caso clássico é um caso particular deste.

A porta quântica Hadamard ou simplesmente H, largamente utilizada para gerar superposições de estados, é comumente descrita pela sua representação matricial:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3.4}$$

A aplicação de H aos estados da base computacional $|0\rangle$ e $|1\rangle$ gera superposições igualmente distribuídas onde a probabilidade de se obter um dos estados ao se fazer uma medição no qubit é a mesma, 50%:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{e} \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

A porta de fase S introduz uma fase relativa $e^{i\pi/2} = i$ (onde $i = \sqrt{-1}$) no estado do qubit, ou seja, aplicada a um estado genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $S|\psi\rangle = \alpha|0\rangle + i\beta|1\rangle$. A matriz que representa S é :

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix} \tag{3.5}$$

Outras portas quânticas elementares são representadas pelas matrizes abaixo :

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad e \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{3.6}$$

As portas quânticas apresentadas acima operam sobre o estado de um qubit e a informação associada está no nível quântico. Para torná-la acessível no nível clássico precisamos realizar uma medição. Então, é necessário introduzir uma porta de medição M para representar a operação de medição do estado de um qubit. O efeito desta porta é projetar o estado do qubit em um dos estados da base $|0\rangle$ ou $|1\rangle$ apresentando como resultado um valor aleatório 0 ou 1, respectivamente.

Exercício 3.2: Mostre que as matrizes que representam as portas quânticas X, Y, Z, H, S e I apresentadas acima são unitárias.

Exercício 3.3: Mostre que as portas quânticas X, Y, Z, H, S e I apresentadas acima são reversíveis.

3.2.3 Circuitos quânticos

Um circuito quântico é um dispositivo que consiste de portas quânticas conectadas umas as outras e cujos passos computacionais são sincronizados no tempo. Como os circuitos lógicos clássicos, os circuitos quânticos são mais comumente apresentados e entendidos através de um gráfico ou diagrama. A Figura 3.4 apresenta o diagrama de um circuito consistindo de duas aplicações sucessivas da porta H a um qubit :

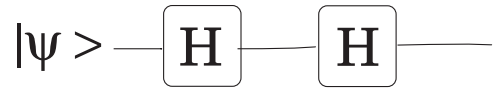

Figura 3.4: Circuito com duas portas Hadamard e um qubit, representando a operação : $HH|\psi\rangle = H^2|\psi\rangle$.

A entrada do circuito é o vetor de estado de um qubit ($|\psi\rangle$), as linhas horizontais são análogas aos fios de um circuito clássico e representam a evolução (da esquerda

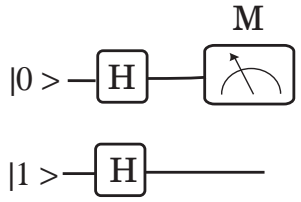

Figura 3.5: Circuito com dois qubits

para direita) do estado do qubit (passagem do tempo ou deslocamento de uma partícula) e a saída é o novo vetor de estado do qubit após a aplicação sucessiva das portas H, $H^2|\psi\rangle$.

A Figura 3.5 apresenta um circuito cuja entrada consiste de dois qubits nos estados iniciais $|0\rangle$ e $|1\rangle$, respectivamemente, de duas portas Hadamards aplicadas uma a cada qubit e de uma porta de medição M aplicada ao primeiro qubit. A saída do circuito é o estado dos dois qubits após a aplicação das operações indicadas : $|0\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ ou $|1\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, dependendo do resultado da medida do primeiro qubit. Sem a porta de medição, o estado do sistema na saída do circuito seria : $(|0\rangle + |1\rangle)/\sqrt{2}\ (|0\rangle - |1\rangle)/\sqrt{2} = (|00\rangle - |01\rangle + |10\rangle - |11\rangle)/2$.

A ação do circuito da Figura 3.6 pode ser descrita como :

$$\begin{aligned}(H \otimes H)(|0\rangle|0\rangle) &= H^{\otimes 2}|00\rangle = H|0\rangle \otimes H|0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |01\rangle + |11\rangle) \qquad (3.7)\end{aligned}$$

Na notação decimal:

$$= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

Ou seja, o circuito produz uma superposição igualmente distribuída de todos os estados da base computacional do espaço dos dois qubits, $\mathbb{C}^2 \otimes \mathbb{C}^2$. A notação $H \otimes H$ ou $H^{\otimes 2}$ significa o *produto tensorial* do operador (ou matriz) H com ele mesmo.

Generalizando para circuitos com n qubits, obtemos:

$$\begin{aligned}H^{\otimes n}|0\ldots 0\rangle &= (H|0\rangle)^{\otimes n} \\ &= (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle))^{\otimes n} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \qquad (3.8)\end{aligned}$$

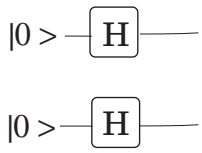

Figura 3.6: Circuito para gerar a superposição de estados da base computacional.

com o circuito apresentado na Figura 3.7 abaixo :

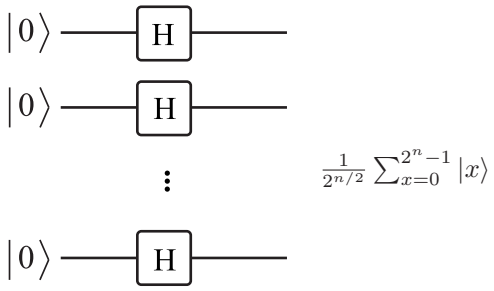

Figura 3.7: Circuito para obter a superposição de estados da base computacional que põe registrador no estado $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$.

Exercício 3.4: Monte e teste os circuitos apresentados acima utilizando o simulador Zeno.

3.2.4 Porta CNOT

Em geral, podemos usar as portas quânticas de 1-qubit para transformar o estado $|0\ldots0\rangle$ de n qubits em qualquer estado do tipo $|\psi_1\rangle|\psi_2\rangle\ldots|\psi_n\rangle$, onde cada $|\psi_i\rangle$ é uma superposição arbitrária $\alpha|0\rangle + \beta|1\rangle$. Porém, esses estados que podem ser obtidos por um conjunto de portas básicas sobre um número fixado de qubits são estados do tipo produto-direto (ou separáveis). Para se obter estados emaranhados, precisamos de portas (ou operações) sobre múltiplos qubits .

A porta CNOT (ou porta NOT-controlada) é uma porta multiqubit aplicada ao estado de dois qubits (controle e alvo) e sua ação pode ser definida pelas transformações operadas nos estados da base computacional associada, ou seja:

$$\begin{aligned} |00\rangle &\longrightarrow |00\rangle \\ |01\rangle &\longrightarrow |01\rangle \\ |10\rangle &\longrightarrow |11\rangle \\ |11\rangle &\longrightarrow |10\rangle \end{aligned} \tag{3.9}$$

Isto é, se o bit de controle (o primeiro) estiver no estado $|0\rangle$, nada acontece ao alvo (o segundo). Porém, se o qubit de controle estive no estado $|1\rangle$, a operação X é aplicada ao estado do qubit alvo. A Figura 3.8 abaixo apresenta o diagrama da porta CNOT :

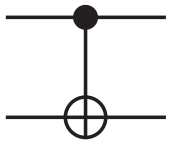

Figura 3.8: Porta CNOT.

A matriz associada à porta CNOT é a seguinte :

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.10}$$

Duas maneiras convenientes de representar a ação da porta CNOT sobre os estados da base computacional são :

$$|i, j\rangle \rightarrow |i, i \oplus j\rangle \tag{3.11}$$

onde $i, j \in \{0, 1\}$ e $\oplus$ é a operação soma módulo 2, e

$$|i, j\rangle \rightarrow |i\rangle X^i |j\rangle \tag{3.12}$$

onde X^i indica a aplicação i vezes da porta X.

Podemos generalizar a porta NOT-controlada para uma porta U-controlada onde U é uma operação unitária qualquer sobe um qubit e cuja ação pode ser dada pelo diagrama da Figura 3.9.

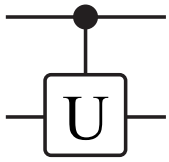

Figura 3.9: Porta U-controlada.

Um resultado importante sobre circuitos quânticos é que o conjunto de portas de 1-qubit mais a porta C-NOT é *universal*, ou seja, qualquer operação unitária pode ser representada por um circuito quântico composto apenas de portas desse conjunto.

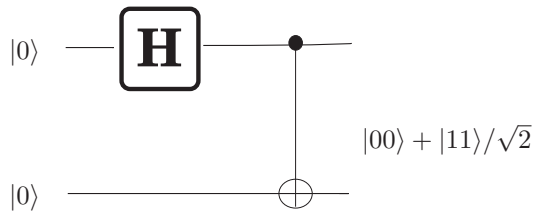

Figura 3.10: Circuito que produz um estado emaranhado de dois qubits

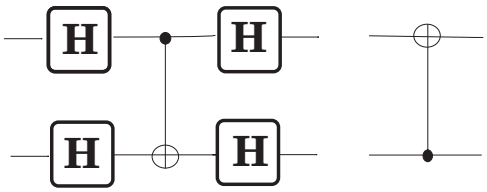

Figura 3.11: Equivalência entre os circuitos.

Utilizando a porta H e a porta CNOT podemos construir um circuito que produz um estado emaranhado de dois qubits mostrado na Figura 3.10.

Exercício 3.5 : Mostre que a matriz U_{CNOT} é unitária.

Exercício 3.6 : Mostre que a matriz U_{CNOT} é sua própria inversa

Exercício 3.7 : Mostre e teste a porta CNOT no simulador Zeno, tanto como matriz 4×4 quanto utilizando a porta X e um controle.

Exercício 3.8 : Mostre e teste no simulador Zeno como implementar a porta SWAP, utilizando apenas CNOT's, cuja função é trocar o estado de $2 - qubits$, ou seja, SWAP$|x\rangle|y\rangle = |y\rangle|x\rangle$.

Exercício 3.9 : Mostre que a porta CNOT não pode ser obtida a partir de portas de $1 - qubit$

Exercício 3.10 : Mostre que os dois circuitos da Figura 3.11 são equivalentes.

3.2.5 Computação quântica

Uma operação quântica é unitária e portanto reversível. Então, um computador quântico precisa de dois registradores para realizar uma computação: um para guardar o estado da entrada e outro para o estado da saída. A computação de uma função f seria determinada por uma operação unitária U_f que agiria sobre os dois

registradores preservando a entrada, de acordo com o seguinte protocolo :

$$U_f|x\rangle|y\rangle \;=\; |x\rangle|y \oplus f(x)\rangle \tag{3.13}$$

Podemos observar que, se $y = 0$, então,

$$U_f|x\rangle|0\rangle \;=\; |x\rangle|0 \oplus f(x)\rangle \;=\; |x\rangle|f(x)\rangle \tag{3.14}$$

Suponha que preparamos um registrador com m qubits no estado $|\psi\rangle$ de superposição igualmente distribuída, conforme a equação (3.8), e um registrador com n qubits no estado $|0\rangle$, ou seja :

$$|\psi\rangle|0\rangle \;=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^m-1} |x\rangle|0\rangle \tag{3.15}$$

Aplicando U_f ao estado $|\psi\rangle|0\rangle$, como mostra o circuito da Figura 3.12, obtemos:

$$\begin{aligned} U_f|x\rangle|0\rangle &= U_f\left(\frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle|0\rangle\right) \\ &= \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} U_f|x\rangle|0\rangle \\ &= \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle|f(x)\rangle \end{aligned} \tag{3.16}$$

Ou seja, o circuito realiza a computação de todos os 2^m valores $f(0), f(1), \ldots, f(2^{m-1})$ ao mesmo tempo com uma única aplicação da operação unitária U_f que implementa a função f. Essa característica incomum de calcular todos os valores de f ao mesmo tempo é chamada paralelismo quântico. No entanto, esse paralelismo por si só não se concretiza em vantagem pois essa informação está no nível quântico e ao medir o estado do registrador de saída obtemos apenas o valor da função em um ponto e que não reflete toda informação contida na superposição.

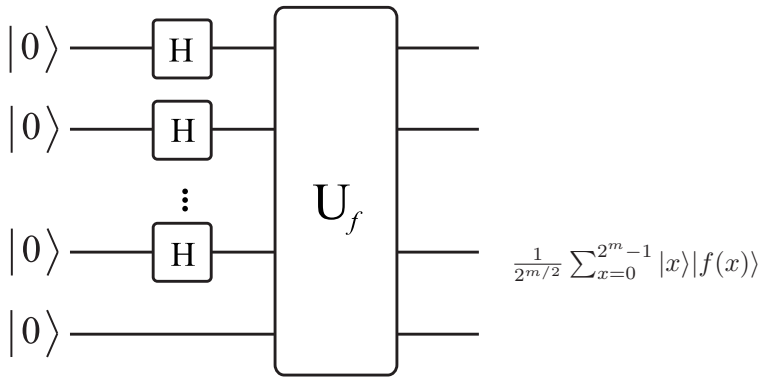

Figura 3.12: Computando valor de f para todos os valores de x.

Capítulo 4

O algoritmo de Deutsch

4.1 O problema de Deutsch

O primeiro exemplo concreto de utilização de operações quânticas para realizar uma computação foi o algoritmo quântico conhecido como o *algoritmo de Deustch*, apresentado por David Deutsch em 1985. O problema a resolver é o seguinte : suponha que seja dada uma "caixa preta"ou "oráculo"que computa uma função booleana $f : \{0,1\} \rightarrow \{0,1\}$ desconhecida. Como sabemos, existem 4 dessas funções, conforme tabela 4.1 abaixo:

As funções f_0 e f_3 são chamadas funções *constantes*, ou seja, $f_i(0) = f_i(1)$, e as funções f_1 e f_2 são chamadas funções *balanceadas*.

O problema consiste em determinar qual é o tipo de função que o oráculo implementa, constante ou balanceada, com o mínimo de consulta ao oráculo. Classicamente, precisaríamos consultar o oráculo duas vezes para calcular os valores de $f(0)$ e $f(1)$ e então comparar esses valores para extrair a informação desejada. Uma maneira de realizar essa comparação é, por exemplo, calcular a soma módulo 2 de $f(0)$ com $f(1)$:

$$f(0) \oplus f(1) = \begin{cases} 0 \text{ se } f \text{ é constante} \\ 1 \text{ se } f \text{ é balanceada} \end{cases}$$

pois $0 \oplus 0 = 0$, $1 \oplus 1 = 0$, $0 \oplus 1 = 1$ e $1 \oplus 0 = 1$.

Deustch mostrou que é possível determinar que tipo de função consultando o oráculo apenas uma vez, fazendo uso da superposição e interferência quânticas.

função	$x = 0$	$x = 1$
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

Tabela 4.1: Tabela representado as possíveis funções booleanas $f : \{0,1\} \rightarrow \{0,1\}$

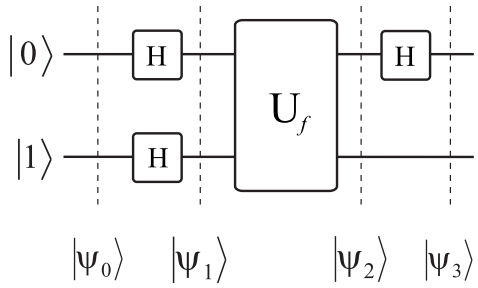

Figura 4.1: Circuito de Deutsch

Circuito da Figura 4.1 implementa uma variante do algoritmo quântico de Deustch. O estado de entrada do circuito é $|\psi_0\rangle = |01\rangle$ e a porta unitária U_f implementa o oráculo :

Depois da aplicação das duas portas H, o estado do sistema $|\psi_1\rangle$ será :

$$|\psi_1\rangle \;=\; \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{4.1}$$

Note que aplicando U_f a um dado estado $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, obteremos:

$$\begin{aligned} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &\xrightarrow{U_f} |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\ &= \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{se } f(x) = 0 \\ |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} & \text{se } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{4.2}$$

A partir daí, não é difícil mostrar que, ao aplicarmos U_f a $|\psi_1\rangle$ teremos as seguintes possibilidades:

$$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) = f(1) \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) \neq f(1) \end{cases} \tag{4.3}$$

Aplicando-se uma porta H ao primeiro qubit, teremos:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) = f(1) \\ \pm|1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) \neq f(1) \end{cases} \tag{4.4}$$

que podemos reescrever da seguinte forma:

$$|\psi_3\rangle = \pm(|f(0) \oplus f(1)\rangle) \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{4.5}$$

Assim, o estado do primeiro qubit contém a informação desejada sobre a função : $f(0) \oplus f(1)$. Fazendo uma medição no primeiro qubit saberemos se a função é constante ou balanceada.

Observe que a expressão (4.3) pode ser reescrita como (omitindo os fatores de normalização para facilitar o entendimento):

$$\begin{aligned}
&\sum_{x=0,1} (-1)^{f(x)}|x\rangle \, (\, |0\rangle - |1\rangle \,) \\
&\qquad = \Big[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big] \, (\, |0\rangle - |1\rangle \,) \\
&\qquad = (-1)^{f(0)} \Big[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\Big] \, (\, |0\rangle - |1\rangle \,) \qquad (4.6)
\end{aligned}$$

ou seja, a aplicação de U_f ao estado $|\psi_1\rangle = (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$ tem o efeito de deixar inalterado o estado do segundo qubit mas introduz um fator de fase no estado do primeiro qubit igual a $(-1)^{f(0)\oplus f(1)}$ (o fator de fase global $(-1)^{f(0)}$ não tem significado e pode ser desprezado). É justamente nesse fator de fase que está a informação desejada sobre a função f : se f é constante, $f(0) \oplus f(1) = 0$, $(-1)^{f(0)\oplus f(1)} = 1$ e o estado do primeiro qubit será portanto $(|0\rangle + |1\rangle)$. A aplicação posterior de H à esse qubit resultará no estado $|0\rangle$. Por outro lado, se f é balanceada, $f(0) \oplus f(1) = 1$, $(-1)^{f(0)\oplus f(1)} = -1$ e o estado do primeiro qubit será portanto $(|0\rangle - |1\rangle)$. A aplicação posterior de H a esse qubit resultará no estado $|1\rangle$.

Assim, o papel principal da operação U_f no circuito é gerar o fator de fase relativa no estado do primeiro qubit [ver (4.6)] de acordo com o tipo de f implementado. O segundo qubit tem a função de *auxiliar* nesse processo.

Podemos ver, portanto, que o acesso à informação desejada que relaciona os possíveis valores da função f implementada só é possível graças à superposição e à interferência. A superposição possibilita o cálculo dos valores da função de maneira simultânea, e a interferência é o ingrediente chave na solução do problema de Deutsch fazendo com que a propriedade desejada seja apresentada como um fator de fase relativa entre os estados.

4.2 O algoritmo de Deutsch e o interferômetro de Mach-Zehnder

Com base nas discussões sobre o algoritmo de Deutsch e sobre o inteferômetro de Mach-Zehnder,em seções anteriores, podemos agora analisar e comentar o papel dos elementos (portas) do circuito de Deutsch e sua relação com os dispositivos óticos (espelhos defasadores) do interferômetro. Para tal, vamos seguir passo a passo a execução do algoritmo em paralelo com o funcionamento do interferômetro, de acordo com as Figuras 1.5 e 4.1, respectivamente. Nos passos a seguir omitiremos os fatores de normalização e fases globais para simplificar a notação :

1º **passo do algoritmo** : criar superposições dos estados de entrada

$$|0\rangle|1\rangle \xrightarrow{H\otimes H} (|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \tag{4.7}$$

Ou seja, o primeiro qubit inicialmente no estado $|0\rangle$ é colocado no estado de superposição $|0\rangle + |1\rangle$ pela primeira porta H e o segundo qubit é colocado no estado $|0\rangle - |1\rangle$ pela segunda porta H. Esse estado servirá como auxiliar no passo seguinte de geração do fator de fase desejado.

1º **passo do interferômetro** : usar ES_1 para criar superposição de caminhos

$$|0\rangle \xrightarrow{ES_1} (|0\rangle + i|1\rangle) \tag{4.8}$$

Podemos ver que a função de ES_1 é similar à da primeira porta H (Hadamard) do circuito : criar uma superposição dos caminhos $|0\rangle$ e $|1\rangle$. Podemos observar que na expressão (4.8) aparece, pelo efeito de ES_1, um fator i no caminho $|1\rangle$. Entretanto, para facilitar a análise podemos desconsiderá-lo e continuar a rotular esse caminho por $|1\rangle$ visto que o fator i não produz efeito observável nos detectores [ver expressão (1.12)]. Assim, podemos reescrever a expressão (4.8) na forma

$$|0\rangle \xrightarrow{ES_1} (|0\rangle + |1\rangle) \tag{4.9}$$

2º **passo do algoritmo**: gerar fator de fase

$$\begin{aligned}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{U_f} &(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \\ &(|0\rangle - |1\rangle)\end{aligned} \tag{4.10}$$

Ou seja, U_f deixa inalterado o segundo qubit e introduz o fator de fase relativa $(-1)^{f(0)\oplus f(1)}$ no primeiro qubit. O segundo qubit pode então ser desprezado.

2º **passo do interferômetro** : defasar os caminhos $|0\rangle$ e $|1\rangle$ por ϕ_0 e ϕ_1

$$\begin{aligned}(|0\rangle + |1\rangle) \xrightarrow{E_0,\phi_0,E_1,\phi_1} &e^{i\phi_0}|1\rangle + e^{i\phi_1}|0\rangle \\ &|0\rangle + e^{i(\phi_0-\phi_1)}|1\rangle\end{aligned} \tag{4.11}$$

Os defasadores introduzem um fator de fase relativa entre os percursos igual a $e^{i(\phi_0-\phi_1)}$. Para que esse defasamento nos caminhos simule o fator de fase relativa $(-1)^{f(0)\oplus f(1)}$ introduzido por U_f no circuito de Deutsch, $e^{i(\phi_0-\phi_1)} = (-1)^{f(0)\oplus f(1)}$, o que implica em :

$$(\phi_0 - \phi_1) = \begin{cases} 0 & \text{para o caso } f(0) = f(1) \\ \pi & \text{para o caso } f(0) \neq f(1) \end{cases} \tag{4.12}$$

Isto é, os defasadores devem ser preparados tais que $(\phi_0 - \phi_1) = 0$, se o interferômetro deve simular aplicação do algoritmo de Deutsch a uma função constante, ou tais que $(\phi_0 - \phi_1) = \pi$, no caso de uma função balanceada.

3º **passo do algoritmo** :

$$(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \xrightarrow{H}[(1 + (-1)^{f(0)\oplus f(1)})|0\rangle + \\ +(1 - (-1)^{f(0)\oplus f(1)})|1\rangle]/2 \tag{4.13}$$

Ou seja, a porta H remete o estado do primeiro qubit para $|0\rangle$, se $f(0) \oplus f(1) = 0$ (função constante), ou para $|1\rangle$ se $f(0) \oplus f(1) = 1$ (função balanceada). Uma medição do qubit indicará uma das duas situações com certeza absoluta.

3º **passo do interferômetro** : ES_2 recombina os percursos

$$|0\rangle + e^{i\phi}|1\rangle \xrightarrow{ES_2} \cos(\phi/2)|0\rangle + i\text{sen}(\phi/2)|1\rangle \tag{4.14}$$

onde $\phi = (\phi_0 - \phi_1)$. Note que ES_2 tem função análoga à última porta H do circuito : recombina os percursos de maneira que o feixe (fóton) saia pelo caminho $|0\rangle$ e seja detectado pelo detector D_0, se $\phi = 0$, ou saia pelo caminho $|1\rangle$ e seja detectado pelo detector D_1, se $\phi = \pi$. O interferômetro é portanto capaz de determinar com precisão absoluta a fase relativa entre os caminhos, desde que ela seja 0 ou π.

Como vemos, cada passo do algoritmo corresponde exatamente à passagem do fóton por um dispositivo óptico do interferômetro e as descrições matemáticas correspondentes são equivalentes, ou seja,o interferômetro de Mach-Zehnder tem a mesma estrutura matemática do algoritmo de Deutsch.

4.3 O algoritmo de Deutsch-Jozsa

O algoritmo original de Deutsch foi subseqüentemente generalizado pra funções booleanas de aridade n qualquer, $f : \{0,1\}^n \to \{0,1\}$. As funções são assumidas serem constantes ou balanceadas (isto é, o número de entradas para as quais a função tem valor 0 é igual ao número de entradas para as quais a função tem valor 1) e o objetivo é determinar se a função que o oráculo computa é constante ou balanceada, com o mínimo de consultas ao oráculo.

Classicamente, esse problema requer, no pior caso, $O(2^n)$ consultas para se determinar com certeza a resposta correta. O algoritmo de Deutsch-Jozsa descrito, abaixo resolve este problema com uma única consulta ao oráculo :

Analisando o circuito :

$$\begin{aligned} |\psi_1\rangle &= \left(H^{\otimes n} \otimes H\right)\left(|0\rangle_n|1\rangle\right) \\ &= \left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{x=0}^{2^n-1}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right)\right) \end{aligned} \tag{4.15}$$

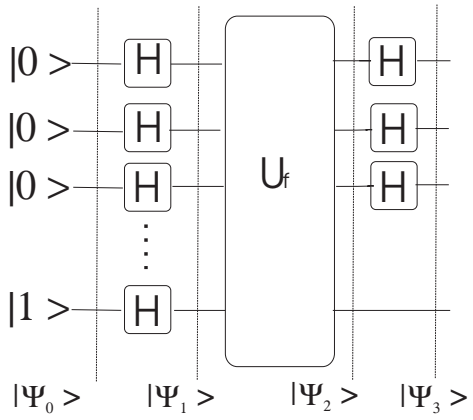

Figura 4.2: Circuito de Deutsch-Jozsa

e

$$\begin{aligned}
|\psi_2\rangle &= U_f\,|\psi_1\rangle \\
&= U_f\left(\frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{x=0}^{2^n-1}(\,|x\rangle|0\rangle - |x\rangle|1\rangle\,)\right)\right) \\
&= \frac{1}{2^{n/2}\sqrt{2}}\left(U_f\left(\sum_{x=0}^{2^n-1}|x\rangle|0\rangle\right) - U_f\left(\sum_{y=0}^{2^n-1}|y\rangle|1\rangle\right)\right) \\
&= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle - \sum_{y=0}^{2^n-1}|y\rangle|\overline{f(y)}\rangle\right) \qquad (4.16)
\end{aligned}$$

Se f é constante temos dois casos :

1. $f(x) = 0$ para todo $x \in \{0,1\}^n$.

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle - \sum_{y=0}^{2^n-1}|y\rangle|\overline{f(y)}\rangle\right) \\
&= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{z=0}^{2^n-1}|z\rangle\,(|0\rangle - |1\rangle\,)\right) \\
&= \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}|z\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \qquad (4.17)
\end{aligned}$$

2. $f(x) = 1$, para todo $x \in \{0,1\}^n$

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle - \sum_{y=0}^{2^n-1}|y\rangle|\overline{f(y)}\rangle\right) \\
&= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{z=0}^{2^n-1}|z\rangle\left(|1\rangle - |0\rangle\right)\right) \\
&= -\frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}|z\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \qquad (4.18)
\end{aligned}
$$

ou seja :

$$
|\psi_2\rangle = \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}(-1)^{f(z)}|z\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)
$$

Se f é balanceada :

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2^{n/2}\sqrt{2}}\left(\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle - \sum_{y=0}^{2^n-1}|y\rangle|\overline{f(y)}\rangle\right) \\
&= \frac{1}{2^{n/2}\sqrt{2}}\left(\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \ldots + |2^n-1\rangle|f(2^n-1)\rangle\right) - \right. \\
&- \left.\left(|0\rangle|\overline{f(0)}\rangle + |1\rangle\overline{f(1)} + \ldots + |2^n-1\rangle|\overline{f(2^n-1)}\rangle\right)\right) \\
&= \frac{1}{2^{n/2}}\sqrt{2}\sum_{z=0}^{2^n-1}|z\rangle\left(|f(z)\rangle - |\overline{f(z)}\rangle\right) \\
&= \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}|z\rangle\left(\frac{|f(z) - |\overline{f(z)}\rangle\rangle}{\sqrt{2}}\right) \qquad (4.19)
\end{aligned}
$$

como para metade dos termos $f(z) = 0$ e para a outra metade $f(z) = 1$:

$$
|\psi_2\rangle = \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}(-1)^{f(z)}|z\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)
$$

$$
\begin{aligned}
|\psi_3\rangle &= \left(H^{\otimes n} \otimes \mathbf{I}\right) |\psi_2\rangle \\
&= \left(H^{\otimes n} \otimes \mathbf{I}\right) \left(\frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{f(z)} |z\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= H^{\otimes n} \left(\frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{f(z)} |z\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{2^{n/2}} \left(H^{\otimes n}((-1)^{f(0)}|0\rangle) + \ldots + H^{\otimes n}((-1)^{f(2^n-1)}|2^n-1\rangle) \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{2^{n/2}} \left((-1)^{f(0)} H^{\otimes n}|0\rangle + \ldots + (-1)^{f(2^n-1)} H^{\otimes n}|2^n-1\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{2^{n/2}} \left(\frac{(-1)^{f(0)}}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{0\cdot z} |z\rangle + \ldots + \frac{(-1)^{f(2^n-1)}}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{(2^n-1)\cdot z} |z\rangle \right) \\
&= \frac{1}{2^n} \left(\sum_{z=0}^{2^n-1} (-1)^{f(0)} (-1)^{0\cdot z} |z\rangle + \ldots + \sum_{z=0}^{2^n-1} (-1)^{f(2^n-1)} (-1)^{(2^n-1)\cdot z} |z\rangle \right) \\
&= \frac{1}{2^n} \left(\sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{y\cdot x + f(y)} |x\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \qquad (4.20)
\end{aligned}
$$

A amplitude a_0 do componente $|0\rangle$ do estado do 1º registrador é :

$$a_0 = \sum_{y=0}^{2^n-1} \frac{(-1)^{f(y)}}{2^n}$$

Se f é constante, então $f(y) = 0$ ou $f(y) = 1$, para todo $y \in \{0, 1\}$. Então,

$$
\begin{aligned}
f(y) &= 0 \quad \Rightarrow \quad \sum_{y=0}^{2^n-1} \frac{(-1)^{f(y)}}{2^n} = 1 \\
f(y) &= 1 \quad \Rightarrow \quad \sum_{y=0}^{2^n-1} \frac{(-1)^{f(y)}}{2^n} = -1 \qquad (4.21)
\end{aligned}
$$

Então, como $|\psi_3\rangle$ é um estado normalizado, a única amplitude diferente de zero é a amplitude de $|0\rangle$, a_0. Uma medição nos n qubits do registrador 1 encontrará os n qubits no estado $|0\rangle$, com 100% de certeza.

Se f é balanceada, uma medição deve produzir um resultado diferente de zero.

Capítulo 5

Transformada de Fourier quântica e funções periódicas

5.1 Transformada de Fourier

A transformada de Fourier tem um grande número de aplicações em muitos ramos da ciência. Às vezes, é mais fácil encontrar uma solução para a versão transformada de Fourier de um problema do que para sua versão original. Na computação quântica, a transformada de Fourier tem se constituído em uma ferramenta fundamental na maioria dos algoritmos quânticos mais conhecidos e importantes como os algoritmos de Shor para a fatoração e logaritmos discretos.

A transformada discreta de Fourier clássica (DFT) pode ser vista como uma transformação de um vetor de N números complexos $\vec{x} = (x_0, x_1, \ldots, x_{N-1})$ em um outro vetor de complexos da mesma dimensão $\vec{y} = (y_0, y_1, ..., y_{N-1})$, e que vamos denotar por $DFT(\vec{x}) = \vec{y}$, cuja ação sobre os componentes é descrita por :

$$y_k \;=\; \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} x_j \tag{5.1}$$

Exemplo : Seja $N = 2$ e $\vec{x} = (1, 0)$, então $\vec{y} = DFT(\vec{x}) = (1/\sqrt{2}, 1/\sqrt{2})$.

A transformada de Fourier discreta quântica (QFT) é definida analogamente como uma transformação linear sobre uma base ortonormal $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ cuja ação sobre os estados da base é descrita por :

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle \tag{5.2}$$

Exemplo : Seja $N = 2$ (1 qubit). Então, $QFT(|0\rangle) = (|0\rangle + |1\rangle)/\sqrt{2}$ e $QFT(|1\rangle) = (|0\rangle - |1\rangle)/\sqrt{2}$.

A representação da QFT em produto exterior (matriz) poder ser obtida da seguinte forma :

$$\begin{aligned}
QFT &= \mathbf{I}\cdot QFT\cdot\mathbf{I} \\
&= \sum_{j=0}^{N-1}|j\rangle\langle j|\cdot QFT\cdot\sum_{k=0}^{N-1}|k\rangle\langle k| \\
&= \sum_{j,k=0}^{N-1}|j\rangle\langle j|\cdot QFT\cdot|k\rangle\langle k| \\
&= \sum_{j,k=0}^{N-1}\langle j|QFT|k\rangle\,|j\rangle\langle k| \\
&= \sum_{j,k}\langle j|\left(\frac{1}{\sqrt{N}}\sum_{d=0}^{N-1}e^{i2\pi kd/N}|d\rangle\right)|j\rangle\langle k| \\
&= \frac{1}{\sqrt{N}}\sum_{j,k=0}^{N-1}\langle j|\sum_{d=0}^{N-1}e^{i2\pi kd/N}|d\rangle|j\rangle\langle k| \\
&= \frac{1}{\sqrt{N}}\sum_{j,k=0}^{N-1}e^{i2\pi kd/N}|j\rangle\langle k| \qquad (5.3)
\end{aligned}$$

Como QFT é uma transformação linear, então, se sabemos como ela atua nos estados da base computacional, também sabemos como ela atua num estado genérico de n qubits $|\psi\rangle$:

$$QFT(|\psi\rangle) = QFT\left(\sum_{j=0}^{N-1}\alpha_j|j\rangle\right) = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\sum_{k=0}^{N-1}\alpha_j e^{i2\pi jk/N}|k\rangle \qquad (5.4)$$

Exercício 5.1: Obtenha as matrizes da QFT para 2 e 3 qubits.

Exercício 5.2: Mostre que a QFT é unitária .

Exercício 5.3: Seja $N = 4$ (2 qubits) . Calcule a QFT dos estados da base computacional.

Exercício 5.4: Seja $|\psi_k\rangle = QFT(|k\rangle)$ e $B = \{|\psi_k\rangle : 0 \leq k \leq N-1\}$. Mostre que os elementos de B formam uma base ortonormal, isto é, $\langle\psi_{k'}|\psi_k\rangle = \delta_{k,k'}$.

Exercício 5.5: Monte e teste o circuito da QFT com quatro qubits usando o simulador Zeno.

O custo computacional da transformada de Fourier dada pelas equações 5.1 ou 5.2 aplicada a um vetor de dimensão N é da ordem $\Theta(N^2) = \Theta(2^{2^n})$. Podemos obter um algoritmo mais eficiente fazendo as seguintes transformações :

1. Convertendo o $|k\rangle$ em 5.2 para a base 2 e usando a expansão de k em potências de 2 no expoente, obtemos:

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi i j \sum_{m=1}^{n} k_m/2^m} |k_1\rangle \dots |k_n\rangle \tag{5.5}$$

2. Considerando que o exponencial da soma é o produto das exponenciais :

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \prod_{m=1}^{n} e^{2\pi i j k_m/2^m} |k_m\rangle \tag{5.6}$$

3. Trocando a soma pelo produto :

$$\begin{aligned} QFT(|j\rangle) &= \frac{1}{\sqrt{N}} \prod_{m=1}^{n} \sum_{k_m=0}^{1} e^{2\pi i j k_m/2^m} |k_m\rangle \\ &= \frac{1}{\sqrt{N}} \prod_{m=1}^{n} (|0\rangle + e^{2\pi i j/2^m} |1\rangle) \end{aligned} \tag{5.7}$$

que podemos escrever como :

$$QFT(|j\rangle) = \left(\frac{|0\rangle + e^{2\pi i j/2^1} |1\rangle}{\sqrt{2}} \right) \otimes \dots \otimes \left(\frac{|0\rangle + e^{2\pi i j/2^n} |1\rangle}{\sqrt{2}} \right) \tag{5.8}$$

A equação 5.8 implica num custo computacional menor,da ordem $\Theta(n2^n)$, porém ainda exponencial. No entanto, ela enseja um algoritmo polinomial da ordem de $\Theta(n^2)$ para o cálculo da transformada discreta de Fourier quântica, cujo circuito é apresentado na figura abaixo

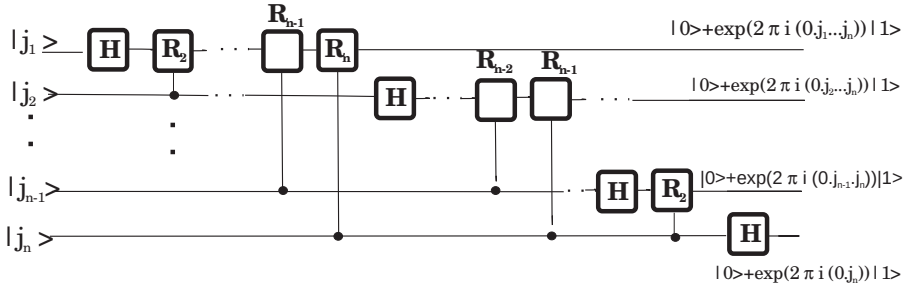

Figura 5.1: Circuito quântico para transformada discreta de Fourier

A porta R_k denota a transformação unitária

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{5.9}$$

Para mostrar que o circuito acima computa QFT, considere o que acontece quando temos o estado $|j_1\rangle, \ldots, |j_n\rangle$ na entrada. A porta Hadamard aplicada ao primeiro qubit produz o resultado :

$$\frac{|0\rangle + e^{2\pi i 0.j_1}|1\rangle}{\sqrt{2}} |j_1\rangle \ldots |j_n\rangle,$$

visto que $e^{2\pi i 0.j_1} = -1$ quando $j_1 = 1$ e 1 quando $j_1 = 0$. Aplicando em seguida a porta R_2-controlada obtemos o estado $((|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)\sqrt{2})\,|j_2\rangle \ldots |j_n\rangle$. Continuando a aplicar sucessivamente as portas R_3-controlada, R_4-controlada até R_n-controlada, cada uma das quais adiciona um bit extra na fase do coeficiente do primeiro $|1\rangle$, obtemos o estado :

$$\frac{|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle}{\sqrt{2}} |j_2 j_3 \ldots j_n\rangle.$$

Aplicando um procedimento similar ao estado do segundo qubit vamos obter o estado :

$$\frac{(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{\sqrt{2}} \frac{(|0\rangle + e^{2\pi i 0.j_2 j_3 \ldots j_n}|1\rangle)}{\sqrt{2}} |j_3 j_4 \ldots j_n\rangle$$

Continuando desta maneira para cada qubit,obtemos o estado:

$$\frac{(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{\sqrt{2}} \frac{(|0\rangle + e^{2\pi i 0.j_2 j_3 \ldots j_n}|1\rangle)}{\sqrt{2}} \cdots \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)}{\sqrt{2}}$$

Invertendo os qubits através da utilização de portas SWAP,obtemos finalmente o estado :

$$\frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)}{\sqrt{2}} \cdots \frac{(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle)}{\sqrt{2}} \frac{(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{\sqrt{2}}$$

que é precisamente a equação 5.8 para a transformada discreta de Fourier.

O número de portas utilizadas por esse circuito pode ser contabilizado como segue: inicialmente é aplicada uma porta Hadamard e $n-1$ portas R_k-controladas ao primeiro qubit dando um total de n portas. A seguir, é aplicada uma porta Hadamard e n-2 portas R_k-controladas ao segundo qubit, dando um total parcial de n+(n-1) portas. Continuando dessa forma, vamos chegar a um total de n(n+1)/2 portas. Adicionando neste total as n/2 portas SWAP requeridas para as inversões e sabendo que cada porta SWAP pode ser implantada a partir de 3 portas CNOT, chegamos a um total da ordem de $\Theta(n^2)$ portas para implementar a transformada discreta de Fourier através de um circuito ou algoritmo quântico.

5.2 Transformada de Fourier e Período de uma função

A eficiência de algoritmos quânticos, tais como os algoritmos de Shor para fatoração e logaritmo discreto, vem diretamente da eficiência de algoritmos quânticos para determinar o período de uma dada *função periódica*.

Seja a função, $f : \{0, 1, \ldots, N-1\} \rightarrow \mathbb{Z}$, que é garantidamente periódica para algum período r, $1 \leq r < N$:

$$f(x + r) = f(x), \quad \text{para todo} \quad x \in \mathbb{Z}_N.$$

onde $\mathbb{Z}_N$ denota o grupo de inteiros módulo N, a adição é módulo N e r divide N. Temos uma caixa preta que computa f eficientemente.
Problema : determinar r.

Caso Clássico

Na ausência de qualquer outra informação sobre f, podemos meramente consultar o oráculo para diferentes valores de r até encontrar 2 valores que são mapeados no mesmo valor de f. Isto nos dá alguma informação sobre r, o que leva o custo para encontrar r ser, no pior caso, da ordem de $O(N)$.

Caso Quântico

O circuito quântico da figura 5.2 determina o período da função com apenas uma consulta ao oráculo U_f.

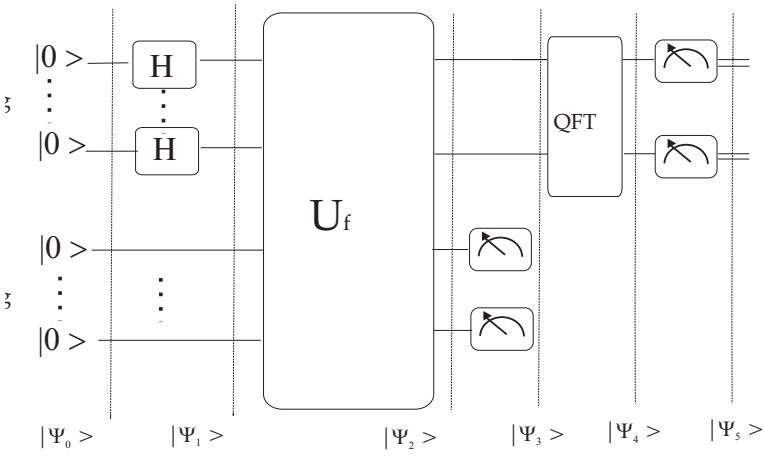

Figura 5.2: Circuito quântico para calcular o período de uma função

Análise do Circuito

$$\begin{aligned} |\psi_0\rangle &= |0\rangle|0\rangle \\ |\psi_1\rangle &= \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|0\rangle \\ |\psi_2\rangle &= \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|f(x)\rangle \end{aligned} \tag{5.10}$$

Exemplo: $f(x) = 3^x \bmod 16$

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{4}\left(|0\rangle|1\rangle + |1\rangle|3\rangle + |2\rangle|9\rangle + |3\rangle|11\rangle\right. \\ &+ |4\rangle|1\rangle + |5\rangle|3\rangle + |6\rangle|9\rangle + |7\rangle|11\rangle \\ &+ |8\rangle|1\rangle + |9\rangle|3\rangle + |10\rangle|9\rangle + |11\rangle|11\rangle \\ &+ \left.|12\rangle|1\rangle + |13\rangle|3\rangle + |14\rangle|9\rangle + |15\rangle|11\rangle\right) \end{aligned} \tag{5.11}$$

Medindo o 2^{o} registrador e tendo como resultado o valor y_0 digamos, então o estado do 1^{o} registrador será reduzido a uma superposição igualmente distribuída de todos os $|x\rangle$'s tais que $f(x) = y_0$. Se x_0 é o menor de tais x´s e como $N = K.r$ (r divide N), então :

$$|\psi_3\rangle = \frac{1}{\sqrt{K}}\sum_{j=0}^{K-1}|x_0 + j.r\rangle|y_0\rangle \tag{5.12}$$

com $0 \leq x_0 < r - 1$.

Assim:

y_0	$\lvert\psi_3\rangle$	x_0
1	$\frac{1}{2}(\lvert 0\rangle + \lvert 4\rangle + \lvert 8\rangle + \lvert 12\rangle)\lvert 1\rangle$	0
3	$\frac{1}{2}(\lvert 11\rangle + \lvert 5\rangle + \lvert 9\rangle + \lvert 13\rangle)\lvert 3\rangle$	1
9	$\frac{1}{2}(\lvert 2\rangle + \lvert 6\rangle + \lvert 10\rangle + \lvert 14\rangle)\lvert 9\rangle$	2
11	$\frac{1}{2}(\lvert 13\rangle + \lvert 7\rangle + \lvert 11\rangle + \lvert 15\rangle)\lvert 11\rangle$	3

A figura 5.3 mostra a distribuição de probabilidade de obtermos os estados da base computacional, medindo o primeiro registrador em 5.12.

OBS. x_0 é aleatório pois depende do valor de y_0 obtido pela medição no segundo registrador que é aleatória. Então, como obter r a partir de $|\psi_3\rangle$?

$$|\psi_3\rangle = \frac{1}{\sqrt{N/r}}\sum_{k=0}^{N/r-1}|x_0 + k.r\rangle|y_0\rangle \tag{5.13}$$

Uma maneira seria :

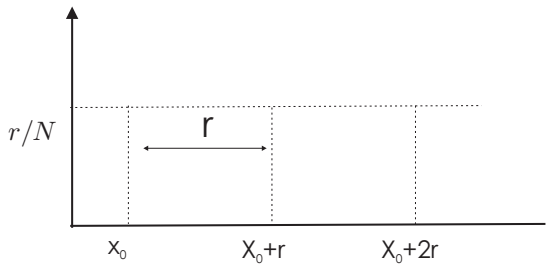

Figura 5.3: Distribuição de probabilidades obtidas pela medição do primeiro registrador em $|\psi_3\rangle$

1. realizar uma medição no primeiro registrador e obter com igual probabilidade qualquer dos valores $x_0, x_0 + r, \ldots, x_0 + N.r$
2. repetir o procedimento do começo e reter apenas as vezes para as quais a saída medida do segundo registrador for o mesmo y_0, medindo então o primeiro registrador.
3. Depois de obter mais de dois valores distintos do primeiro, obter r via o cálculo do mdc entre eles

Problema:

Como x_0 é aleatório, esse procedimento leva a um custo de obtenção de r de ordem $O(N)$.

Usando a QFT($\mathcal{F}$):

$$QFT(|k\rangle) = \mathcal{F}(|k\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{i2\pi jk/N} |j\rangle \tag{5.14}$$

Considerando apenas o primeiro registrador para simplificar :

$$|\psi_3\rangle = \frac{1}{\sqrt{N/r}} \sum_{k=0}^{N/r-1} |x_0 + k.r\rangle \tag{5.15}$$

$$
\begin{aligned}
|\psi_4\rangle &= \mathcal{F}(|\psi_3\rangle) = \frac{1}{\sqrt{N/r}}\left(\mathcal{F}(|x_0+0.r\rangle)+\mathcal{F}(|x_0+1.r\rangle)+\ldots+\mathcal{F}(|x_0+(N/r-1).r\rangle)\right)\\
&= \frac{1}{\sqrt{N/r}}\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{i2\pi(x_0+0.r)j/N}|j\rangle+\ldots+\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{i2\pi(x_0+(N/r-1).r)j/N}|j\rangle\right)\\
&= \frac{1}{\sqrt{N/r}}\frac{1}{\sqrt{N}}\sum_{y=0}^{N/r-1}\sum_{j=0}^{N-1} e^{i2\pi(x_0+y.r)j/N}|j\rangle\\
&= \frac{1}{\sqrt{r}}\sum_{j=0}^{N-1}\frac{1}{N/r}\sum_{y=0}^{N/r-1} e^{i2\pi(x_0+y.r)j/N}|j\rangle\\
&= \frac{1}{\sqrt{r}}\sum_{j=0}^{N-1}\frac{1}{N/r}\sum_{y=0}^{N/r-1} e^{i2\pi x_0 j/N}\cdot e^{i2\pi yrj/N}|j\rangle\\
&= \frac{1}{\sqrt{r}}\sum_{j=0}^{N-1}\left[\frac{1}{N/r}\sum_{y=0}^{N/r-1} e^{i2\pi yrj/N}\right] e^{i2\pi x_0 j/N}|j\rangle \qquad (5.16)
\end{aligned}
$$

A expressão entre colchetes em 5.16 é diferente de zero se, e somente se, $j = b.N/r$ onde $b = 0,\ldots,r-1$. Quando j assume tais valores a expressão entre colchetes é igual a um. Então,

$$|\psi_4\rangle = \frac{1}{\sqrt{r}}\sum_{b=0}^{r-1} e^{i2\pi x_0 b/r}|bN/r\rangle \qquad (5.17)$$

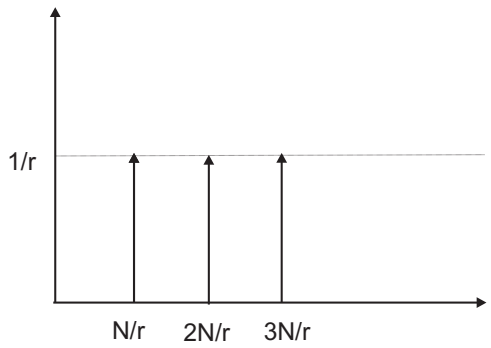

Figura 5.4: Distribuição de probabilidades obtidas pela medição do primeiro registrador em $|\psi_4\rangle$

OBS: x_0 não aparece mais nos rótulos dos kets.

A Figura 5.4 mostra a distribuição de probabilidades de obtermos os estados da base computacional medindo o primeiro registrador em $|\psi_4\rangle$.

Medindo agora o primeiro registrador vamos obter um múltiplo de N/r, isto é, $c_0 = b_0 N/r$. Dividindo c_0 por N :

$$\frac{c_0}{N} = \frac{b_0}{r}$$

onde c_0 e N são conhecidos e $0 \leq b_0 \leq r-1$ é obtido aleatoriamente como resultado da medição. Se b_0 e r são coprimos (isto é, b_0 e r não têm fatores comuns), podemos determinar r reduzindo c_0/N a uma fração irredutível. Se b_0 e r não são coprimos, rodamos novamente o algoritmo até encontrar um valor de c tal que o valor de b correspondente seja coprimo com r. Qual é então a probabilidade de b e r serem coprimos? Não é difícil verificar que essa probabilidade é de no mínimo $1/\log r$ que é maior que $1/\log N$. Portanto, se repetirmos o algoritmo $O(\log N)$ vezes nós podemos determinar r com probabilidade $1-\epsilon$ tão próxima de um quanto desejado.

No caso em que r não divide N, o procedimento é mesmo porém, será necessário aplicar o método de frações continuadas para se obter r.

Exercício 5.6 : Defina, monte e teste no simulador Zeno, um circuito quântico que computa a função $f(x) = 3^x \text{mod} 16$.

Exercício 5.7 : Defina, monte e teste no simulador Zeno, um circuito quântico que compute o período da função definida no exercício 5.6.

Bibliografia

[1] Feynman, R.P., R.B.Leighton and Sands, M., *The Feynman Lectures on Physics*, vol.3, Addison-Wesley, 1965.

[2] Pessoa Junior,O., *Conceitos de Física Quântica*, Editora Livraria da Física, São Paulo, 2003.

[3] Nussenzveig, H.M., Ótica, Relatividade, Física Quântica, *Curso de Física Básica* vol.4, Editora Edgard Blucher LTDA. 1ªed. 1998.

[4] Cabral, G.E.M., Lula Jr., B. and Lima, A. F., Interpretando o algoritmo de Deutsch no interferômetro de Mach-Zehnder, *Revista Brasileira de Ensino de Física*, **26**(2004), 109-116.

[5] Cabral, G.E.M., Lula Jr., B. and Lima, A. F., Zeno a new graphical tool for design and simulation of quantum circuits, *In Proceedings of SPIE, conference Quantum Information and Computation III*, Donkor, E.J., Pirich A.R. and Brandt, H.E., (Eds.), **5815**, 127-137 (2005).

[6] Deutsch, D.,Quantum computational networks , *In Proceedings of the Royal Society of London. Series A*, **425** (1989), 73-90.

[7] Deutsch, D., Quantum theory, the Church-Turing principle and the universal quantum computer, *In Proceedings of the Royal Society of London. Series A*, **400** (1985), 97-117.

[8] Deutsch, D. and Jozsa, R., Rapid Solution of problems by quantum computation, *In Proceedings of the Royal Society of London. Series A*, **439** (1992), 553-558.

[9] Nielsen, M.A. and Chuang, I.L., *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge, 2000.

[10] Preskill, J., *Quantum information and computation*, Lectures Notes, California Institute of Technology, unpublished 1998.

[11] Mermin, D., *Lectures Notes on Quantum Computation*, Lectures Notes, Cornell University, unpublished 2004.

[12] Portugal, R., Lavor, C. C., Carvalho, L. M. and Maculan, N., *Uma Introdução à Computação Quântica* , Notas em Matemática Aplicada, SBMAC, 2004, São Carlos.

[13] Bouwmeester, D. and Zeilinger, A., The Physics of Quantum Information: Basic Concepts, *The Physics of Quantum Information*, Bouwmeester, D., Ekert, A. and Zeilinger, A. (Eds.), Springer Verlag, 1-14, 2000.

[14] Deutsch, D. and Ekert, A., Introduction to Quantum Computation, *The Physics of Quantum Information*, Bouwmeester, D., Ekert, A. and Zeilinger, A. (Eds.), Springer Verlag, 93-103, 2000.

[15] Jozsa, R., Quantum Algorithms, *The Physics of Quantum Information*, Bouwmeester, D., Ekert, A. and Zeilinger, A. (Eds.), Springer Verlag, 104-126, 2000.

[16] Barenco, A., Quantum Computation, *Introduction to Quantum Computation and Information*, Lo,H.-K., Popescu, S. and Spiller, T.(Eds.),World Scientific Publishing, 143-183, 1998.

[17] Williams, C.P. and Clearwater, S.H., *Explorations in Quantum Computing*, Springer Verlag, 1998.

[18] Ekert, A., Hayden, P. and Inamori, H., Basic concepts in quantum computation,*quant-ph archive, quant-ph/0011013*,(2000).