Revista Brasileira de Ensino de Física, v. 26, n. 2, p. 109 - 116, (2004)
www.sbfisica.org.br

Interpretando o algoritmo de Deutsch no interferômetro de Mach-Zehnder

(Interpreting Deutsch's algorithm on the Mach-Zehnder interferometer)

Gustavo Eulalio M. Cabral[1], Aércio Ferreira de Lima[2] e Bernardo Lula Jr.[3]

[1]*Departamento de Sistemas e Computação, Universidade Federal de Campina Grande*
[2]*Departamento de Física, Universidade Federal de Campina Grande*
[3]*Departamento de Sistemas e Computação, Universidade Federal de Campina Grande*
Recebido em 21/11/03; Revisado em 18/03/04; Aceito em 26/04/04

A Computação Quântica é uma área de pesquisa relativamente recente, que vem sendo desenvolvida nos últimos 20 anos, e que faz uso dos fundamentos da Ciência da Computação e da Física Quântica. Dois são os fenômenos quânticos em que se baseia a Computação Quântica: *superposição* e *interferência*. Neste trabalho, destacaremos o papel da interferência na solução do problema proposto por Deutsch, o qual consiste em saber se uma dada função é constante ou balanceada, calculando a função apenas uma vez. Figurativamente, isto equivale a saber se uma moeda é honesta ou viciada (duas faces iguais) olhando-a uma única vez. A solução de Deutsch (algoritmo) é, com freqüência, explicada de forma abstrata e com auxílio de circuitos. Contudo, embora eficiente para expressar a "lógica" e facilitar o desenvolvimento de algoritmos quânticos, esta abordagem não deixa transparecer e facilmente apreender os fenômenos físicos subjacentes. Neste trabalho mostramos didaticamente como o interferômetro de Mach-Zehnder implementa o algoritmo de Deutsch, destacando desta forma a importância da interferência na realização de algoritmos quânticos.
Palavras-chave: algoritmo de Deutsch, interferômetro de Mach-Zehnder, computação quântica.

Quantum Computation is a relatively new research area, which has been in development in the past 20 years, and which makes use of the fundamentals of Computer Science and Quantum Physics. Two are the quantum phenomena in which Quantum Computation is based: *superposition* and *interference*. In this work, we will highlight the role of interference in the solution of the problem proposed by Deutsch, which consists of knowing if a given function is constant or balanced, executing the function only once. Figuratively, this is the same as knowing if a coin is honest or faked (two equal faces) looking only once. Deutsch's solution (algorithm) is frequently explained in an abstract manner and with the help of circuits. However, although efficient to express the "logics" and facilitate the development of quantum algorithms, that approach does not make it clear and easy to realize the underlying physical phenomena. In this work, we show, in a didatic way, how the Mach-Zehnder interferometer implements Deutsch's algorithm, thus highlighting the importance of interference in the realization of quantum algorithms.
Keywords: Deutsch algorithm, Mach-Zehnder interferometer, quantum computation.

1. Introdução

A utilização de fenômenos quânticos para a representação e processamento de informação é uma séria possibilidade para futuras gerações de dispositivos computacionais. As vantagens teóricas advindas dessa utilização vêm atraindo atenção crescente tanto da área científica quanto da área tecnológica/industrial.

Em 1985, Deutsch propôs um algoritmo, utilizando apenas operações quânticas, capaz de resolver um determinado problema matemático impossível de ser resolvido por operações ou métodos clássicos [1]. No entanto, esse algoritmo passou despercebido até 1989, quando Deutsch introduziu a noção de portas lógicas quânticas que poderiam ser conectadas umas às outras formando um circuito ou malha quântica [2].

O algoritmo de Deutsch reescrito na nova linguagem teve a partir de então uma ampla repercussão, pois a linguagem dos qubits (análogo quântico ao *bit* clássico) e portas lógicas quânticas era similar à linguagem de circuitos lógicos/digitais convencionais e poderia ser mais facilmente entendida por engenheiros eletricistas e cientistas da Computação. Daí em diante, outros algoritmos quânticos foram desenvolvidos e difundidos utilizando-se a linguagem matemática associada à linguagem de circuitos quânticos.

Contudo, esse aparato descritivo e interpretativo, embora eficiente para expressar a "lógica" e facilitar o desenvolvimento de algoritmos quânticos, não deixa transparecer e facilmente apreender os fenômenos físicos subjacentes. Um desses fenômenos, a ser explorado neste texto, é a *interferência quântica*. O entendimento

[1]Enviar correspondência para Gustavo Eulálio M. Cabral. E-mail: guga@dsc.ufcg.edu.br.

deste fenômeno é fundamental para se adquirir uma base sólida para a perfeita compreensão das operações e dos resultados que podem ser obtidos por um algoritmo quântico. Nesse artigo, apresentamos, inicialmente, uma breve introdução à linguagem de circuitos quânticos e uma descrição nessa linguagem do algoritmo de Deutsch. Em seguida, apresentamos o fenômeno da interferência através da descrição de um experimento utilizando o interferômetro de Mach-Zehnder. Por fim, apresentamos uma interpretação do algoritmo de Deutsch à luz do experimento.

2. Noções básicas

No que se segue, vamos apresentar as noções básicas e os conceitos fundamentais da Computação Quântica, fazendo sempre o contraponto com as noções e conceitos básicos da Computação Clássica já conhecidos.

2.1. Representação da informação

Na Computação Quântica, ao invés da noção clássica de bit, temos a noção de *qubit* (*quantum bit*). Diferentemente de um bit de informação, que pode estar em (ou representar) apenas dois estados distintos, 0 ou 1, um qubit, além dos estados $|0\rangle$ e $|1\rangle$, pode estar em qualquer *superposição* de estados da forma:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \tag{1}$$

onde c_0 e c_1 são coeficientes complexos e tais que $|c_0|^2 + |c_1|^2 = 1$. As notações $|0\rangle$ e $|1\rangle$ representam, respectivamente, os vetores:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad\qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \tag{2}$$

e a notação $|\psi\rangle$ representa o vetor:

$$|\psi\rangle = \begin{bmatrix}c_0\\c_1\end{bmatrix} \tag{3}$$

Um qubit pode ser realizado de diversas formas: por meio de uma partícula de *spin* $-1/2$, onde os estados $|0\rangle$ e $|1\rangle$ corresponderiam, respectivamente, aos estados *spin-down* e *spin-up*; ou ainda por meio de caminhos seguidos pelo feixe (ou pelo fóton) ao passar por um *beam splitter* (um divisor de feixes). Embora um qubit possa ser preparado em um número infinito de estados quânticos (c_0 e c_1 são complexos), quando medido, só podemos obter um bit de informação. A medição de um qubit inicialmente em um estado $c_0|0\rangle + c_1|1\rangle$ dará como resultado o bit 0, com probabilidade $|c_0|^2$, ou o bit 1, com probabilidade $|c_1|^2$, ou seja, num aparato de medição, os resultados 0 e 1 seriam registrados com uma probabilidade de $|c_0|^2$ e $|c_1|^2$ nos respectivos detectores. Depois de uma medição, ao contrário de um bit clássico que mantém o seu estado, o estado de um qubit é alterado para o estado $|0\rangle$ ou $|1\rangle$, de acordo com as respectivas probabilidades. Ou seja, medir um qubit altera, em geral, seu estado.

Em um computador clássico, bits são agrupados em conjuntos chamados *registradores*. Então, se um bit pode armazenar um dos dois números 0 ou 1, um registrador de n bits pode armazenar 2^n números diferentes ($\{0, 1, ..., 2^n - 1\}$), um por vez.

Em um computador quântico, um registrador de n qubits, por sua vez, pode armazenar 2^n números diferentes ao mesmo tempo. Por exemplo, com 2 qubits podemos representar o estado:

$$\begin{aligned}
|\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\
&= (c_0^{(1)}|0\rangle + c_1^{(1)}|1\rangle) \otimes (c_0^{(2)}|0\rangle + c_1^{(2)}|1\rangle) \\
&= c_0^{(1)}c_0^{(2)}|0\rangle \otimes |0\rangle + c_0^{(1)}c_1^{(2)}|0\rangle \otimes |1\rangle + \\
&\quad\ c_1^{(1)}c_0^{(2)}|1\rangle \otimes |0\rangle + c_1^{(1)}c_1^{(2)}|1\rangle \otimes |1\rangle \\
&\equiv c_0^{(1)}c_0^{(2)}|0\rangle|0\rangle + c_0^{(1)}c_1^{(2)}|0\rangle|1\rangle + \\
&\quad\ c_1^{(1)}c_0^{(2)}|1\rangle|0\rangle + c_1^{(1)}c_1^{(2)}|1\rangle|1\rangle \qquad (4) \\
&\equiv c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + c_3|3\rangle \qquad (5) \\
&= \sum_{x=0}^{3} c_x|x\rangle \qquad (6)
\end{aligned}$$

onde $c_i^{(j)}$ indica o coeficiente c_i do qubit j, e a Equação (5) é obtida da Equação (4) pela mudança da notação binária pela decimal (por exemplo, $|1\rangle|1\rangle$ por $|3\rangle$).

2.2. Processamento da informação

Em um computador clássico, o processamento da informação é realizado por dispositivos chamados de *circuitos lógicos*, que são agrupamentos de dispositivos mais simples conhecidos por *portas lógicas*. Uma porta lógica opera sobre o estado dos bits da entrada, obtendo um outro estado na saída correspondendo à sua "tabela da verdade". Por exemplo, a porta lógica NOT inverte na saída o estado do bit da entrada ($\overline{a} = 1 - a$): se o bit da entrada (a) estiver no estado 0, então o bit 1 é gerado na saída ($\overline{a}$), e vice-versa. A porta AND tem dois bits na entrada (a e b) e gera uma saída, c, dada por $c = a \cdot b$. Com as portas lógicas NOT e AND é possível construir circuitos lógicos capazes de computar qualquer função $f : \{0, ..., 2^m - 1\} \longrightarrow \{0, ..., 2^n - 1\}$ teoricamente computável [3]. Representando as portas NOT e AND como na Figura 1

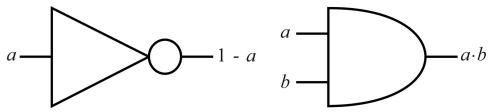

Figura 1 - Portas NOT e AND, respectivamente.

e conectando as portas umas às outras por fios, podemos representar os circuitos lógicos através de um diagrama. Por exemplo, o diagrama da Figura 2 representa um circuito lógico que realiza (ou computa) a função $f(a, b) = a \oplus b$, onde $\oplus$ é a operação adição módulo 2 (**mod 2**) [18].

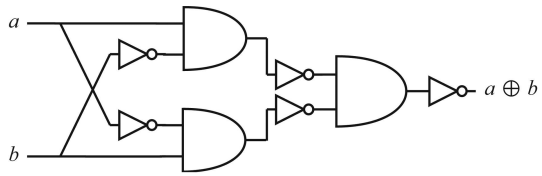

Figura 2 - Circuito que computa a função adição módulo 2.

2.3. Portas de um simples qubit

Em um computador quântico o processo é similar, ou seja, podemos construir (teoricamente) circuitos quânticos, que são agrupamentos de dispositivos mais simples chamados *portas quânticas*, que realizam *operações unitárias* sobre um registrador quântico. Uma porta quântica simples aplica uma operação unitária U (definida por uma matriz unitária 2×2) [19] sobre um qubit no estado $|\psi\rangle$ fazendo-o evoluir para o estado $U|\psi\rangle$. Por exemplo, a porta quântica X, descrita pela matriz:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{7}$$

corresponde à porta lógica NOT:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \tag{8}$$

$$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{9}$$

Nem todas as portas quânticas possuem correspondentes clássicas. Por exemplo, a porta *Hadamard* (ou simplesmente H), definida pela matriz:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{10}$$

leva em estados *sem equivalentes clássicos*. Por exemplo:

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ H|1\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{11}$$

2.4. Portas controladas de dois qubits

As portas X e H são portas quânticas simples que aplicam operações quânticas sobre um único qubit. Apesar do conjunto de portas quânticas simples ser infinito (o número de matrizes unitárias 2×2 é infinito), esse conjunto não é *universal*, ou seja, não é suficiente para construir circuitos quânticos que representam operações quânticas sobre um número n qualquer de qubits (matrizes unitárias $2^n \times 2^n$). Para tanto, é preciso a utilização de portas quânticas de múltiplos qubits cujo representante principal é a porta NOT-controlada ou, como é mais conhecida na literatura, porta CNOT. Esta porta define uma operação sobre 2 qubits a e b (chamados qubit de *controle* e qubit *alvo*, respectivamente) descrita pela matriz 4×4 mostrada abaixo:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{12}$$

e cuja atuação pode ser descrita assim: se o qubit de controle a está no estado $|0\rangle$, o estado do qubit alvo permanece inalterado. Se o qubit de controle a está no estado $|1\rangle$ o estado do qubit alvo é alterado para $|b \oplus a\rangle$. A operação sobre o qubit alvo pode ser expressa como $X^a|b\rangle$, onde X é a porta X e o sobrescrito "a" indica o valor do bit de controle. O diagrama da Figura 3 representa a porta CNOT.

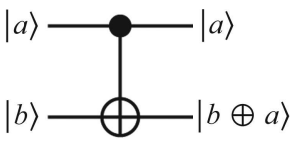

Figura 3 - Porta CNOT.

Podemos generalizar a porta NOT-controlada para uma porta U-controlada sobre dois qubits, onde U é uma operação unitária qualquer sobre um único qubit, e cuja ação é descrita pelo diagrama da Figura 4.

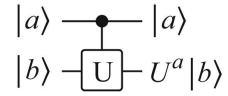

Figura 4 - Porta U-controlada.

O conjunto de portas de um e de dois qubits é universal, ou seja, qualquer operação quântica sobre um número qualquer de qubits pode ser representada por um circuito quântico composto apenas de portas desse conjunto.

2.5. Computação quântica

De acordo com (11), se aplicarmos H a cada um dos qubits de um registrador de n qubits, inicialmente todos no estado $|0\rangle$, obtemos o estado:

$$\begin{aligned} |\psi\rangle &= H \otimes H \otimes \cdots \otimes H|00\ldots0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \\ &\quad \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2^{n/2}}(|00\ldots0\rangle + |00\ldots1\rangle + \cdots + |11\ldots1\rangle) \\ &= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned} \tag{13}$$

Podemos observar que, com um número linear de operações (n aplicações de H), obtemos um estado do registrador que é descrito por um número exponencial de termos distintos (2^n). O circuito quântico da Figura 5 realiza a operação acima descrita (Equação 13). Classicamente, um circuito para computar uma função n-ária [20] f consistiria em um aglomerado de portas com n entradas $x_1, \ldots, x_n$ e uma saída $y = f(x_1, \ldots, x_n)$. Entretanto, um circuito quântico não pode computar uma função dessa forma pois uma operação quântica é unitária e portanto reversível. Um computador quântico precisa de 2 registradores: 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:

$$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle \tag{14}$$

Podemos observar que se y = 0,

$$U_f(|x\rangle|0\rangle) = |x\rangle|0 \oplus f(x)\rangle = |x\rangle|f(x)\rangle \tag{15}$$

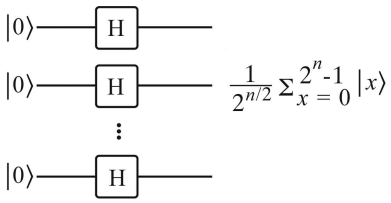

Figura 5 - Circuito que põe registrador no estado $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$.

Agora, suponha que preparamos um registrador quântico $|\psi\rangle$ de m qubits em uma superposição de todos os valores de entrada (2^m) utilizando m portas Hadamard, como na Figura 5. Aplicando U_f a $|\psi\rangle|0\rangle$, como na Figura 6, obtemos:

$$\begin{aligned} U_f(|\psi\rangle|0\rangle) &= U_f\left(\frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle|0\rangle\right) \\ &= \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle|f(x)\rangle \end{aligned} \tag{16}$$

Ou seja, computamos todos os 2^m valores $f(0), f(1), \ldots, f(2^m - 1)$ ao mesmo tempo com uma única aplicação de U_f. A essa característica de poder calcular vários valores de $f(x)$ ao mesmo tempo chamamos de *paralelismo quântico*. O circuito da Figura 6 sintetiza a descrição acima.

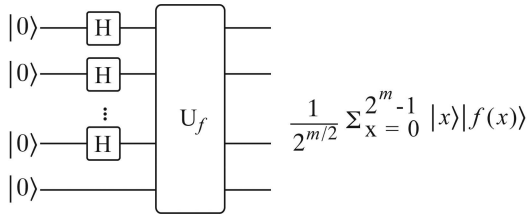

Figura 6 - Computando valor de f para todos os valores de x.

No entanto, este paralelismo por si só não se concretiza em vantagem pois ao medir a saída do circuito (o resultado da computação) obtemos apenas o valor da função em um ponto, que não reflete toda a informação contida na superposição. Uma maneira de se obter uma informação global sobre a função é fazendo uso do fenômeno da interferência, que, junto com o fenômeno da superposição, constitui a base dos atuais algoritmos quânticos.

3. Problema de Deutsch

O problema de Deutsch consiste em saber se uma dada função $f : \{0,1\} \longrightarrow \{0,1\}$ é balanceada ou constante. Existem quatro funções possíveis, como vemos na Tabela 1.

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
0	1	0	0	1
1	1	0	1	0
	constantes		balanceadas	

Tabela 1 - As quatro funções possíveis do tipo $f : \{0,1\} \longrightarrow \{0,1\}$

Classicamente, para saber se f é balanceada ou constante, precisaríamos executá-la 2 vezes, ou seja, calcular os valores de $f(0)$ e de $f(1)$, e compará-los para extrair a propriedade desejada.

Uma maneira de realizar essa comparação é, por exemplo, calcular a soma módulo 2:

$$f(0) \oplus f(1) = \begin{cases} 0 & \text{se } f \text{ é constante} \\ 1 & \text{se } f \text{ é balanceada} \end{cases} \tag{17}$$

pois:

$$\begin{aligned} 0 \oplus 0 = 1 \oplus 1 = 0 \\ 0 \oplus 1 = 1 \oplus 0 = 1 \end{aligned} \tag{18}$$

Quanticamente, é possível resolver este problema executando a função apenas uma vez, fazendo uso do paralelismo e da interferência quântica. O algoritmo apresentado a seguir é uma variante [4] do algoritmo originalmente proposto por Deutsch [1], que faz uso da interferência e do paralelismo e consegue extrair a informação desejada de f, computando-a uma única vez.

3.1. Algoritmo de Deutsch

O circuito da Figura 7 implementa a variante do algoritmo de Deutsch. O estado de entrada do circuito é $|\psi_0\rangle = |01\rangle$.

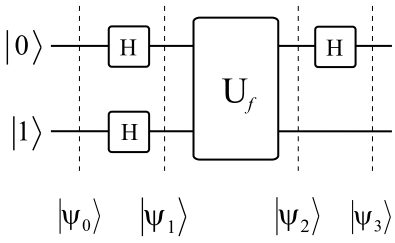

Figura 7 - Circuito de Deutsch.

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

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{19}$$

Note que, como apresentado na seção 2.5, aplicando-se U_f a um dado estado $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, obteremos:

$$\begin{aligned} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{U_f} |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\ = \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{se } f(x) = 0 \\ |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} & \text{se } f(x) = 1 \end{cases} \\ = (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{20}$$

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

$$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) = f(1) \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) \neq f(1) \end{cases} \tag{21}$$

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

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{se } f(0) = f(1) \\ \pm|1\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{se } f(0) \neq f(1) \end{cases} \quad (22)$$

que podemos reescrever da seguinte forma:

$$|\psi_3\rangle = \pm(|f(0) \oplus f(1)\rangle) \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \quad (23)$$

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 (21) pode ser reescrita como (omitindo os fatores de normalização para facilitar o entendimento):

$$\begin{aligned} &\sum_{x=0,1} (-1)^{f(x)}|x\rangle \, (\, |0\rangle - |1\rangle \,) \\ &\quad = \left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right] \, (\, |0\rangle - |1\rangle \,) \\ &\quad = (-1)^{f(0)} \left[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right] \, (\, |0\rangle - |1\rangle \,) \quad (24) \end{aligned}$$

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 a 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 (24)] de acordo com o tipo de f implementado. O segundo qubit tem a função de *auxiliar* nesse processo, conforme detalharemos na seção 5.

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. Interferência

Um dos mais notáveis fenômenos físicos é o fenômeno da interferência. Nas palavras de R. P. Feynman: *"... um fenômeno que é impossível, absolutamente impossível, de explicar de maneira clássica, e que está no coração da mecânica quântica."* [5].

A discussão do fenômeno da interferência é comumente introduzido, nos textos de Física Básica, através do experimento da dupla fenda de Young [6]. Neste experimento, um feixe luminoso atravessa duas fendas existentes em um anteparo opaco. As contribuições ondulatórias provenientes de cada fenda atingem uma tela (detectora), produzindo o conhecido *padrão de interferência*.

Com a disponibilidade tecnológica atual, modernos detectores luminosos e circuitos eletrônicos de alto poder de resolução temporal, é possível construir uma versão moderna do experimento de interferência de Young. Nesta versão moderna, o feixe luminoso será substituído por fótons individuais e o anteparo por foto-detectores.

Será necessário "reinterpretar", à luz da Mecânica Quântica, os elementos constituintes do experimento. Note que, embora um feixe de onda luminoso possa ser separado (através de um espelho semi-transparente) em parte refletida e parte transmitida, um único fóton não é divisível desta maneira. Porém, os caminhos disponíveis (e em princípio indistingüíveis) para o fóton constituem o ingrediente que possibilita o fenômeno da interferência.

Na seção seguinte, são apresentados os componentes básicos e o funcionamento do interferômetro de Mach-Zehnder.

4.1. O Interferômetro de Mach-Zehnder

O interferômetro de Mach-Zehnder poder ser considerado a versão moderna do experimento de dupla fenda de Young [7], onde as fendas no anteparo são substituídas pelos braços do interferômetro (ver Figura 8). Os espelhos semi-transparentes (*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, $R+T = 1$ (ver [8]). E_1 e E_2 são espelhos ($R = 1$ e $T = 0$).

Os defasadores ϕ_0 e ϕ_1 são dispositivos que permitem alterar a fase da onda (moduladores de fase) da maneira desejada. Os dispositivos D_0 e D_1 são detectores da intensidade da onda nas possíveis "saídas".

A intensidade na saída D_0 pode ser obtida (ver [6]) usando os conceitos da Ótica apresentados nas Equações (25) e (26) abaixo:

$$I_{D_0} = \overline{I} \cdot \cos^2\left(\frac{\phi_1 - \phi_2 + k\Delta L}{2}\right) \quad (25)$$

$$I_{D_1} = \overline{I} \cdot sen^2\left(\frac{\phi_1 - \phi_2 + k\Delta L}{2}\right) \quad (26)$$

onde $\overline{I}$ é a intensidade da fonte luminosa, k é o número de onda, e ΔL é a diferença no comprimento dos braços do interferômetro. Embora a discussão acima tenha sido realizada para um feixe de onda incidindo no interferômetro, ela pode ser reinterpretada para o caso de um único fóton incidindo em um dos braços do interferômetro. Uma interessante aplicação deste dispositivo na Criptografia Quântica pode ser encontrada em [9]. Para um descrição detalhada dos elementos de Ótica Quântica, e em particular dos dispositivos aqui discutidos, ver [10]-[12].

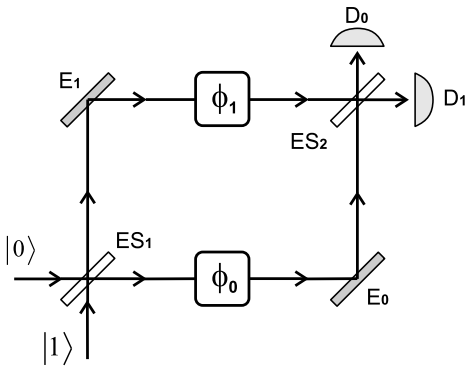

Figura 8 - Visão esquemática do interferômetro de Mach-Zehnder.

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

$$|0\rangle \longrightarrow i\sqrt{R}\,|1\rangle + \sqrt{T}\,|0\rangle \tag{27}$$

ou

$$\begin{aligned} |0\rangle &\longrightarrow i\sqrt{1-T}\,|1\rangle + \sqrt{T}\,|0\rangle \\ |0\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \end{aligned} \tag{28}$$

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.

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

$$\begin{aligned} |1\rangle &\longrightarrow i\sqrt{1-T}\,|0\rangle + \sqrt{T}\,|1\rangle \\ |1\rangle &\longrightarrow \frac{1}{\sqrt{2}}\,i(|0\rangle - i|1\rangle) \end{aligned} \tag{29}$$

Note que o que distingue os estados (28) e (29) 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 por um separador de feixes ES (com $R = T = 1/2$), sobre os caminhos $|0\rangle$ e $|1\rangle$, pode ser representada pela operação unitária U_{ES}

$$U_{ES} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{30}$$

Não é difícil verificar que (30) satisfaz (28-29),

$$\begin{aligned} U_{ES}\,|0\rangle &= \frac{1}{\sqrt{2}}\,(|0\rangle + i|1\rangle) \\ U_{ES}\,|1\rangle &= \frac{i}{\sqrt{2}}\,(|0\rangle - i|1\rangle) \end{aligned} \tag{31}$$

Os espelhos E_1 e E_2 não alteram significativamente os resultados relativos (28-29). O efeito dos espelhos pode ser representado pela operação U_E

$$U_E = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{32}$$

Mais explicitamente,

$$\begin{aligned} U_E|0\rangle &= |1\rangle \\ U_E|1\rangle &= |0\rangle \end{aligned} \tag{33}$$

O caminho seguido pela partícula no interferômetro a partir do seu estado inicial $|0\rangle$ (ver Figura 8) pode agora ser representado por

$$\begin{aligned} |0\rangle \quad &\xrightarrow{ES_1} \quad \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \\ &\xrightarrow{\phi_0, E_0, \phi_1, E_1} \quad \frac{1}{\sqrt{2}}(e^{i\phi_0}|1\rangle + ie^{i\phi_1}|0\rangle) \\ &\longrightarrow \quad ie^{i(\phi_1+\phi_0)/2}\frac{1}{\sqrt{2}}[e^{i(\phi_0-\phi_1)/2}|1\rangle + \\ &\qquad ie^{-i(\phi_0-\phi_1)/2}|0\rangle] \\ &\xrightarrow{ES_2} \quad ie^{i\frac{\phi_0+\phi_1}{2}} \\ &\qquad [\cos\frac{(\phi_0-\phi_1)}{2}\,|0\rangle + \\ &\qquad sen\frac{(\phi_0-\phi_1)}{2}\,|1\rangle\,] \equiv |\Psi_{ES2}\rangle \end{aligned} \tag{34}$$

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

A probabilidade da partícula ser registrada no detector D_0 quando vinda inicialmente pelo caminho "$|0\rangle$" é definida por

$$P_0^{|0\rangle} \equiv |\langle 0|\Psi_{ES_2}\rangle|^2 = \cos^2\frac{(\phi_0-\phi_1)}{2} \tag{35}$$

E para o detector D_1, encontra-se

$$P_1^{|0\rangle} = sen^2\frac{(\phi_0-\phi_1)}{2} \tag{36}$$

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

$$P_0^{|1\rangle} = sen^2\frac{(\phi_0-\phi_1)}{2} \tag{37}$$

e

$$P_1^{|1\rangle} = \cos^2\frac{(\phi_0-\phi_1)}{2} \tag{38}$$

4.2. Algoritmo de Deutsch x interferômetro de Mach-Zehnder

À luz das discussões sobre o algoritmo de Deutsch (seção 3.1), e sobre o interferômetro de Mach-Zehnder (seção 4.1), podemos agora analisar e comentar o papel dos elementos (portas) do circuito de Deutsch e sua relação com os dispositivos óticos (espelhos e 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 Figs. 7 e 8, 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

$$|0\rangle|1\rangle \xrightarrow{H\otimes H} (|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \quad (39)$$

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

$$|0\rangle \xrightarrow{ES_1} (|0\rangle + i|1\rangle) \quad (40)$$

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 (40) 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 (34)]. Assim, podemos reescrever a expressão (40) na forma

$$|0\rangle \xrightarrow{ES_1} (|0\rangle + |1\rangle) \quad (41)$$

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

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{U_f} (|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \\ (|0\rangle - |1\rangle) \quad (42)$$

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

$$(|0\rangle + |1\rangle) \xrightarrow{E_0,\phi_0,E_1,\phi_1} e^{i\phi_0}|1\rangle + e^{i\phi_1}|0\rangle \\ |0\rangle + e^{i(\phi_0-\phi_1)}|1\rangle \quad (43)$$

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 :

$$(\phi_0 - \phi_1) = \begin{cases} 0 & \text{para o caso } f(0) = f(1) \\ \pi & \text{para o caso } f(0) \neq f(1) \end{cases} \quad (44)$$

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** :

$$(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \xrightarrow{H} [(1 + (-1)^{f(0)\oplus f(1)})|0\rangle + \\ + (1 - (-1)^{f(0)\oplus f(1)})|1\rangle]/2 \quad (45)$$

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

$$|0\rangle + e^{i\phi}|1\rangle \xrightarrow{ES_2} \cos(\phi/2)|0\rangle + i\text{sen}(\phi/2)|1\rangle \quad (46)$$

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 ótico do interferômetro e as descrições matemáticas correspondentes são equivalentes, corroborando a afirmação de Cleve et al [4] de que o interferômetro de Mach-Zehnder tem a mesma estrutura matemática do algoritmo de Deutsch.

5. Computação da fase

Como vimos na seção anterior, o ponto chave do algoritmo de Deutsch é a geração do fator de fase relativa $(-1)^{f(0)\oplus f(1)}$ que contém a informação desejada sobre a função f avaliada. Estimar ou avaliar a fase de um estado quântico é equivalente a resolver o problema de encontrar os autovalores de um operador unitário U [21]. Como sabemos, os operadores unitários possuem autovalores λ imaginários puros que podem ser representados por $\lambda = e^{i\phi}$. Ou seja,

$$U|u\rangle = e^{i\phi}|u\rangle \quad (47)$$

O fator de fase $e^{i\phi}$ desejado pode ser computado ou gerado através de uma operação U-controlada (U_c) com o estado do qubit alvo (qubit *auxiliar*) $|u\rangle$ preparado como um auto-estado da operação unitária U, conforme Figura 9.

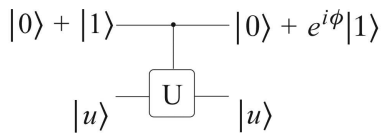

Figura 9 - circuito de computação da fase.

Ou seja,

$$(|0\rangle + |1\rangle)|u\rangle \xrightarrow{U_c} |0\rangle|u\rangle + |1\rangle U|u\rangle \\ |0\rangle|u\rangle + |1\rangle e^{i\phi}|u\rangle \\ (\,|0\rangle + e^{i\phi}|1\rangle\,)\,|u\rangle \quad (48)$$

Da seção 3.1. podemos ver que o fator de fase gerado $(-1)^{f(0)\oplus f(1)}$ corresponde ao autovalor do estado do qubit auxiliar $(|0\rangle - |1\rangle)$ sob ação da operação U_f que envia $|y\rangle$ para $|y \oplus f(x)\rangle$. Para ver como U_f pode ser implementado para cada uma das funções consideradas [Tabela 1] veja referência [13].

6. Conclusão

O objetivo central deste trabalho foi descrever de forma didática como o interferômetro de Mach-Zehnder implementa o algoritmo de Deutsch, ressaltando o papel da interferência quântica (o princípio físico subjacente à maioria dos algoritmos quânticos existentes) na realização deste algoritmo.

Escolhemos o algoritmo de Deutsch por este ser o mais simples dos algoritmos quânticos existentes e que não tem solução clássica, e que utiliza a interferência quântica como ingrediente fundamental. Foi o primeiro algoritmo quântico a ressaltar as vantagens das regras quânticas de computação sobre as clássicas.

Inicialmente introduzimos o estudo de algoritmos e circuitos quânticos, apresentando a notação e os conceitos básicos necessários à compreensão da Computação Quântica. Em seguida, apresentamos os fundamentos básicos do funcionamento do interferômetro de Mach-Zehnder.

Por fim, mostramos como o interferômetro de Mach-Zehnder possui a mesma estrutura matemática do algoritmo de Deutsch.

Este trabalho faz parte de uma série de textos que o grupo de Computação Quântica da Universidade Federal de Campina Grande está desenvolvendo com o objetivo de incentivar a formação de estudantes e pesquisadores em Computação e Informação Quântica. Entre o material didático já produzido, podemos destacar, entre outros, um tutorial na web sobre Mecânica Quântica [14], monografias sobre Computação Quântica (uma introdução) [15] e Criptografia Clássica e Quântica [16], e um *survey* sobre Simuladores Quânticos [17].

Agradecimentos

Agradecemos aos professores Francisco Marcos de Assis, Herman Martins Gomes e Rubens Viana Ramos pela prestimosa colaboração na revisão deste texto.

Referências

[1] D. Deutsch, in *Proc. R. Soc. Lond.* v. A 400, 97, 1985.

[2] D. Deutsch, in *Proc. R. Soc. Lond.* v. A 425, 73, 1989.

[3] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[4] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, in *Proc. R. Soc. Lond.* v. A 454, 339, 1998.

[5] R.P. Feynman, R.B. Leighton and M. Sands, *The Feynman Lectures on Physics* (Addison-Wesley, 1965), v. 3.

[6] H.M. Nussenzveig, *Física Básica* (Edgard Blücher, 1997), v. 4.

[7] R. Cleve, A. Ekert, L. Henderson, C. Macchiavello and M. Mosca, Complexity **4**, 33 (1998).

[8] C.J. Villas-Boas and N.G. de Almeida, Revista Brasileira do Ensino de Física **22**, 489 (2000).

[9] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. (2002).

[10] L.M. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, 1995).

[11] W. Vogel and D.G. Welsch, *Lectures on Quantum Optics* (Arkademie Verlag, 1994).

[12] D.F. Walls and G.J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).

[13] N.D. Mermin, *Lectures Notes Quantum Computation Physics* (Cornel University, 2003).
Disponível em `http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html`.

[14] C.R.G. Isidro, R.F. Herbster, M.A.H. da Silva, V.S. Vilar, A.R. de Souza and A.R. de Lima. *Tutorial sobre Mecânica Quântica* (2003). Disponível em `http://www.gia.dsc.ufcg.edu.br/pcq/mq/`.

[15] A.F. Lima, B. Lula Jr. and G.E.M. Cabral, *Introdução à Computação Quântica* (Rel. Tec. n.) DSC/002/03, Universidade Federal de Campina Grande, Campina Grande, 2003).

[16] C.R.G. Isidro and B. Lula Jr., *Introdução à Criptografia Clássica e à Criptografia Quântica* (Rel. Tec. n.) DSC/007/03, Universidade Federal de Campina Grande, Campina Grande, 2003.

[17] G.E.M. Cabral and B. Lula Jr., *O Estado da Arte em Ferramentas para Síntese e Simulação de Circuitos Quânticos* (Rel. Tec. n.) DSC/003/03, Universidade Federal de Campina Grande, Campina Grande, 2003.

[18] Na aritmética modular, a operação módulo 2 é definida como o resto r da divisão euclidiana de um número m por 2: $m = k \cdot 2 + r$, onde k é um inteiro. Então, dizemos que $r = m \bmod 2$.

[19] Uma matriz unitária U é toda aquela que satisfaz a seguinte propriedade: $UU^\dagger = I = U^\dagger U$, onde $\dagger$ é a operação transposta conjugada e I é a matriz identidade.

[20] Uma função n-ária é uma função com n entradas

[21] O autovalor λ de um operador A é definido pela equação $A|v\rangle = \lambda|v\rangle$. $|v\rangle$ é chamado auto-estado (ou autovetor) de A. A estimação da fase de um estado qualquer $|v\rangle$ que não seja auto-estado do operador U tem um papel fundamental na maioria dos algoritmos quânticos conhecidos.Para uma discussão detalhada sobre estimação da fase veja [4].