Computação Quântica: O Algoritmo de Deutsch e o Paralelismo Quântico

Fernando Luís Semião da Silva

Instituto de Física Gleb Wataghin, Universidade Estadual de Campinas, Unicamp, 13083-970, Campinas, São Paulo, Brasil
e-mail: semiao@ifi.unicamp.br

Resumo

O objetivo desse artigo é apresentar conceitos básicos sobre computação e informação quântica de modo que o leitor possa tomar contato com essa recente área da física, hoje em desenvolvimento nos principais centros de pesquisa. A computação quântica se diferencia da computação clássica que conhecemos principalmente no modo como as funções são calculadas. No caso quântico, existe um paralelismo decorrente da superposição coerente de estados o que permite a realização de múltiplos cálculos simultâneos da função de interesse. Esse é o assunto abordado nesse artigo, que ainda apresenta o algoritmo de Deutsch o qual fornece uma indicação direta do poder computacional contido na mecânica quântica.

1 Introdução

Quando pensamos em computação é usual que tenhamos uma idéia abstrata baseada em conceitos e argumentos lógicos que estão mais próximos da matemática que da física. Contudo, não podemos nos esquecer que o computador é um *objeto físico* e o processo computacional, seja ele efetuado por qualquer hardware, é um processo que obedece às leis da física. Uma vez que a mecânica quântica é uma teoria fundamental, parece natural pensarmos em uma máquina que realize o processamento de informação num nível tal que a superposição e o emaranhamento de estados quânticos possam ser utilizados como um novo tipo de *recurso computacional*. Essa é a idéia formalizada por Deutsch [1] num artigo que despertou a atenção da comunidade de físicos para essa nova área de pesquisa que reune física, matemática e ciência da computação, e que hoje conhecemos pelo nome de computação quântica.

A procura por sistemas físicos capazes de implementar essas idéias de maneira controlada assume grande importância nessa área. Em [2] é proposto o uso de um íon aprisionado num potencial harmônico interagindo com o campo quantizado de uma cavidade na implementação de um conjunto universal de portas lógicas. Essa proposta apresenta algumas vantagens sobre as demais envolvendo íons porque permite o uso de fótons no envio de informação a pontos distantes do espaço. No que segue são apresentados alguns conceitos básicos sobre computação quântica, incluindo uma importante característica da evolução temporal dos sistemas quânticos que é o *paralelismo*. Essa importante característica será ilustrada no chamado *Algoritmo de Deutsch* também discutido nesse artigo. Não é objetivo discutir aqui questões práticas como, por exemplo, a viabilidade de construção de um computador quântico em grande escala ou características particulares de uma ou outra proposta de implementação. O artigo é dedicado à apresentação de alguns conceitos básicos que dão uma idéia geral da potencialidade da computação quântica. Uma boa introdução ao assunto pode ser encontrada em [3].

2 Qubits e Portas Lógicas

Em computação clássica, a menor unidade de informação, o *bit*, pode assumir dois estados, 0 ou 1. Sua generalização quântica se dá no contexto de sistemas de dois níveis no qual o estado geral (puro) para esse bit quântico, ou *qubit*, é dado por:

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

que é parametrizado por dois números complexos a e b, satisfazendo a relação de normalização $|a|^2 + |b|^2 = 1$.

Vemos que existem infinitas possibilidades para o estado de um qubit, podendo estar numa superposição coerente de 0 e 1. Essa característica dá origem a um paralelismo sem análogo clássico, já explorado na criação de algoritmos quânticos eficientes para solução de problemas de grande complexidade computacional. Um exemplo que ilustra bem a eficência da computação quântica é o problema da fatoração de grandes números inteiros. Esse problema demanda um tempo exponencial de solução no melhor algoritmo clássico conhecido. Foi demonstrado [4] que um computador quântico seria capaz de solucionar esse problema num tempo polinomial, o chamado *algoritmo de Shor*, o que vem motivando a pesquisa em algoritmos quânticos e consolida a espectativa sobre o poder computacional de tais máquinas.

Muitos sistemas físicos podem ser usados como qubits. Os estados $|0\rangle$ e $|1\rangle$ podem corresponder, por exemplo, a duas polarizações distintas de um fóton, ou a dois estados de um spin nuclear num campo magnético uniforme, ou ainda a dois estados de energia de um elétron num átomo. Nesse último caso, iluminando o átomo com luz de energia apropriada, é possível manipular o estado do sistema de modo a promover mudanças de $|0\rangle$ para $|1\rangle$, ou o processo inverso.

A idéia pode ser facilmente generalizada para o caso de múltiplos qubits. Consideremos o caso de dois qubits. Se fossem bits clássicos, teríamos então quatro estados possíveis, 00, 01, 10 e 11. Correspondentemente, um sistema quântico de dois qubits tem uma *base computacional*

com quatro componentes denotadas $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. Um par de qubits podem também existir numa superposição desses quatro estados. Um importante estado de dois qubits é o chamado *estado de Bell* ou *par EPR* dado por:

$$|\psi^{'}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \qquad (2)$$

Esse estado, aparentemente simples, é o responsável por muitas surpresas em computação e informação quântica, incluindo o teletransporte de estados quânticos. O estado de Bell tem a propriedade de que uma medida sobre um dos qubits tem dois resultados possíveis: 0 com probabilidade $1/2$, levando ao estado $|\phi^{'}\rangle = |00\rangle$, e 1 com probabilidade $1/2$, levando ao estado $|\phi^{'}\rangle = |11\rangle$. Assim, uma medida no outro qubit sempre dará o mesmo resultado que a medida no primeiro qubit, isso significa que o resultado das medidas estão *correlacionados*. Ainda mais, outros tipos de medida podem ser realizadas no primeiro, ou segundo qubit, e as correlações entre os resultados das medidas ainda existirão. Essas correlações têm sido objeto de grande interesse desde o famoso artigo de Einstein, Podolsky e Rosen onde eles apontaram pela primeira vez essas estranhas propriedades do estado de Bell [5]. Essas correlações foram estudadas por John Bell [6] que provou um resultado muito interessante e surpreendente: as correlações medidas no estado de Bell são mais fortes que qualquer outra que possa existir nos sistemas clássicos. Esses resultados foram talvez a primeira indicação de que a mecânica quântica permite processamento de informação além do que é possível no mundo clássico. Em [7], é apresentado um esquema de geração de toda uma base de estados desse tipo, utilizando como qubits o estado vibracional de movimento de um íon aprisionado e o estado do campo eletromagnético quantizado.

Operações sobre um qubit devem preservar sua norma, e portanto, devem ser descritas por matrizes unitárias. Em princípio, qualquer operação unitária pode ser imaginada como uma *porta lógica quântica*. No espaço de dimensão 2, ou seja, de um único qubit, o efeito da aplicação de operações unitárias pode ser visualizado como a rotação de um vetor unitário na chamada esfera de Bloch [3], e por esse motivo, operações unitárias em um único qubit são freqüentemente chamadas de rotações de qubits. Uma porta de um qubit que possui importância fundamental nos algoritmos quânticos é a chamada porta de Hadamard. A ação dessa porta na base computacional é dada por:

$$|0\rangle \Longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |1\rangle \Longrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \qquad (3)$$

Essa é uma porta sem análogo clássico pois o resultado final de sua aplicação leva a uma superposição coerente dos dois estados da base computacional, algo não presente na computação clássica que, no máximo, faria uma troca negando o bit de entrada na chamada operação NOT.

3 Paralelismo Quântico

A vantagem de um computador quântico é a maneira como ele calcula funções em paralelo. De modo simplificado, o paralelismo quântico é a capacidade que tais máquinas têm de calcular um função $f(x)$ para muitos diferentes valores de x simultaneamente.

Para entender como isso ocorre, consideremos o caso simples de uma função $f(x) : \{0,1\} \rightarrow \{0,1\}$. Para que a operação seja reversível é conveniente guardar junto ao valor de $f(x)$ o valor da variável x. Isso pode ser feito com a aplicação de uma sequência apropriada de portas lógicas [3], transformando o estado inicial em $|x, y \oplus f(x)\rangle$, no qual o primeiro qubit é registrador de dados e o segundo o registrador alvo. O sinal $\oplus$ denota a operação de soma binária, ou seja, $|y \oplus f(x)\rangle = |0\rangle$ se $y = f(x)$ ou $|y \oplus f(x)\rangle = |1\rangle$ se $y \neq f(x)$. A transformação $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ é usualmente denotada por U_f. No caso $y = 0$ o estado do segundo qubit é exatamente o valor $f(x)$.

Consideremos agora a aplicação de U_f no qubit $(|0\rangle + |1\rangle)/\sqrt{2}$ que não pertence à base computacional. Esse estado pode ser criado com a aplicação da porta de Hadamard (3) em $|0\rangle$. Uma vez que U_f é um operador linear, sua aplicação em $(|0\rangle + |1\rangle)/\sqrt{2}$ resulta no estado $|\psi\rangle$ dado por:

$$|\psi\rangle = U_f \frac{|0,0\rangle + |1,0\rangle}{\sqrt{2}} = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}. \qquad (4)$$

Esse é um estado que contém informação sobre $f(0)$ e $f(1)$. Sua forma sugere que tivemos o cálculo $f(x)$ para dois valores de x simultaneamente. Essa característica é chamada de *paralelismo quântico*. É importante ressaltar que se x puder assumir n valores distintos, então, uma *única* aplicação de U_f calculará a função f para n diferentes valores de x.

Ao contrário do paralelismo clássico onde circuitos múltiplos são construídos para computar simultâneamente $f(x)$, cada um deles para um valor de x, aqui um único circuito quântico é empregado no cálculo da função para diferentes valores de x simultaneamente. Isso é uma conseqüência direta do fato de que um bit quântico pode estar num estado de superposição.

O paralelismo quântico permite que todos os valores da função f sejam calculados simultaneamente, ainda que tenhamos calculado essa função uma única vez. Contudo, esse paralelismo não é imediatamente útil, isso porque uma medida resultará em apenas um único valor da função. Em nosso exemplo, a medida resultará ou no estado $|0, f(0)\rangle$ ou no estado $|1, f(1)\rangle$. Claramente, qualquer computador clássico pode fazer isso muito bem. Deve existir então alguma coisa a mais que torne o paralelismo quântico algo útil, ou seja, algo

que nos permita extrair mais informação de superposições do tipo $\sum_x |x, f(x)\rangle$ do que apenas um único valor $f(x)$. Veremos agora um exemplo de como informação adicional pode ser retirada de problemas desse tipo.

4 O Algoritmo de Deutsch

No intuito de compreender melhor os assuntos discutidos nas seções anteriores, é apresentado agora o chamado algoritmo de Deutsch [1]. Esse combina de forma clara duas propriedades importantes: *paralelismo quântico* e *interferência*, sendo este último efeito, o responsável em tornar o paralelismo útil na obtenção de mais informação sobre a função, isso com ainda apenas um único passo. O estado de entrada (input) é escolhido como:

$$|\psi_0\rangle = |01\rangle. \tag{5}$$

Esse estado é enviado à duas portas de Hadamard o que resulta em:

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{6}$$

Em seguida, esse estado é enviado à porta U_f. Notamos que a aplicação de U_f em estados do tipo $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ resulta em:

$$\begin{aligned} U_f|x\rangle(|0\rangle - |1\rangle)/\sqrt{2} &= \frac{|x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle}{\sqrt{2}} \\ &= |x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \\ &= (-1)^{f(x)}|x\rangle\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}. \end{aligned} \tag{7}$$

Usando esse resultado, obtém-se:

$$\begin{aligned} |\psi_2\rangle = &\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \\ &\frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \end{aligned} \tag{8}$$

ou seja,

$$|\psi_2\rangle = \begin{cases} \pm\left[\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) = f(1), \\ \pm\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) \neq f(1). \end{cases} \tag{9}$$

Uma aplicação final da porta de Hadamard no primeiro qubit resulta em:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) = f(1), \\ \pm|1\rangle\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{se } f(0) \neq f(1). \end{cases} \tag{10}$$

Notando que $f(0) \oplus f(1)$ é igual a zero se $f(0) = f(1)$ e igual a um de outro modo, podemos reescrever (10) concisamente na forma:

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{11}$$

Portanto, medindo o primeiro qubit pode-se então determinar $f(0) \oplus f(1)$. Assim, essa sequência de operações quânticas fornece como resposta uma propriedade global de $f(x)$ que é $f(0) \oplus f(1)$, com apenas um único cálculo da função f. Isso supera qualquer lógica clássica, que exigiria o cálculo de $f(0)$ e $f(1)$ para então realizar a soma.

Esse exemplo ilustra a diferença existente entre o paralelismo quântico e os algoritmos clássicos aleatórios (*randomized algorithms*). O estado $\{|0, f(0)\rangle + |1, f(1)\rangle\}/\sqrt{2}$ **não** corresponde a um computador clássico que calcula $f(0)$ com probabilidade $1/2$ e $f(1)$ também com probabilidade $1/2$, isso porque num computador clássico, essas duas alternativas excluem uma a outra. No caso de um computador quântico é possível que as duas alternativas interfiram entre si para gerar algum tipo de propriedade global da função. Isso é realizado com uso de portas do tipo Hadamard que combinam as diferentes alternativas, como é o caso do algoritmo de Deutsch.

A essência e a dificuldade do desenvolvimento de algoritmos quânticos é justamente a escolha apropriada dos qubits de entrada e da transformação final. Essas escolhas devem permitir uma determinação eficiente de propriedades globais da função de interesse, propriedades essas que requeririam uma maior quantidade de cálculos num computador clássico.

5 Conclusão

Em resumo, a mecânica quântica quando aplicada ao processamento de informação traz recursos computacionais profundamente distintos daqueles já conhecidos na computação clássica. Emaranhamento e superposição coerente de estados têm um papel fundamental no chamado paralelismo quântico. Esse paralelismo consiste na capacidade de tais máquinas calcularem simultaneamente uma função para muitos valores diferentes de entrada. As perguntas que naturalmente surgem são: Quais as dificuldades encontradas na implementação prática dessas idéias? Essas máquinas já existem? De fato, essas idéias exigem um alto grau de controle sobre o sistema quântico escolhido para a manipulação de informação. A interação desse sistema com o resto do

Universo induz perda de coerência na evolução unitária das portas e o estado de saída passa então a não ser exatamente o estado esperado. Essa é uma dificuldade fundamental e o principal motivo dessas máquinas quânticas existirem apenas em pequena escala (alguns poucos qubits). Diversos experimentos já demonstraram o funcionamento de portas lógicas quânticas, mas ainda nenhuma aplicação prática pode ser realizada com tão poucos qubits. Uma revisão de alguns dos principais sistemas físicos potencialmente candidatos a implementação prática desses computadores pode ser encontrada em [3]. Grande parte dos trabalhos nessa área estão disponíveis na base de dados de Los Alamos no site: http://arxiv.org/archive/quant-ph. Essa é uma excelente fonte de informação em computação e informação quântica.

6 Agradecimentos

Eu gostaria de agradecer ao corpo editorial da revista Physicae pelo convite e também à Camila Sanches pelo incentivo e apoio, sem sua ajuda este artigo seria ainda um projeto. Apoio financeiro da FAPESP (Fundação de Amparo a Pesquisa do Pesquisa do Estado de São Paulo).

Referências

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

[2] F. L. Semião, A. Vidiella-Barranco and J. A. Roversi, Phys. Lett. A **299**, 423 (2002).

[3] Michael A. Nielsen, Isaac L. Chuang, *Quantum Computation and Quantum Informação*, Cambridge, 2000.

[4] Peter W. Shor, quant-ph/9508027.

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

[6] J. S. Bell, Rev. Mod Phys. **38**, 447 (1966).

[7] F. L. Semião, A. Vidiella-Barranco and J. A. Roversi, Phys. Rev. A **64**, 024305 (2001).