FUNDAMENTOS DA COMPUTAÇÃO QUÂNTICA

Aluno: David Felice F. Baptista
e-mail: davidfelice.ba@gmail.com
Orientador: Prof. Dr. Romis R. F. Attux
e-mail: attux@dca.fee.unicamp.br
Depto. de Engenharia de Computação e Automação Industrial (DCA) – FEEC/UNICAMP

Palavras Chave: Teoria de Computação - Computação Quântica – Física Moderna

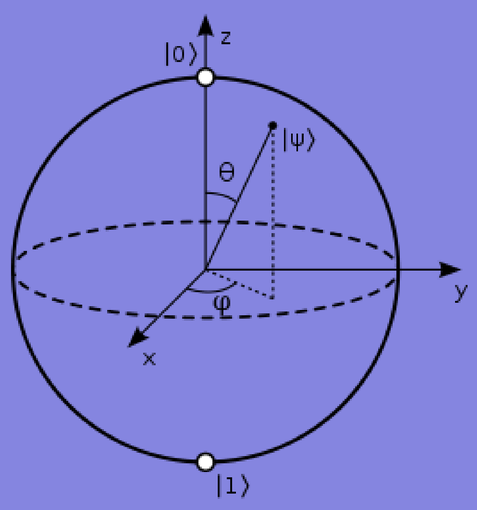
INTRODUÇÃO

Os limites teóricos inerentes à computação digital, cuja investigação foi um assunto abordado de maneira pioneira por Turing, Church e outros, são determinantes para que se estabeleça o potencial tecnológico do mundo moderno. Decorre disso a relevância de buscar alternativas que, eventualmente, transcendam esses limites, permitindo assim o tratamento de problemas atualmente não-computáveis ou não-factíveis. Dentre essas alternativas, vem recebendo grande destaque o paradigma de computação quântica. Nesse trabalho, serão expostas as bases desse paradigma de uma forma sintética e acessível, com o intuito de disseminar o conhecimento sobre a área.

QUBIT

Qubit é a unidade fundamental de informação no contexto do computador quântico.Podemos tecer analogias com a definição clássica de bit, mas é preciso ter em mente algumas diferenças cruciais.

Um *qubit* pode ser representado como um vetor definido num espaço complexo. No caso de dois estados fundamentais (e.g. estados de spin de um elétron), teríamos um *qubit* da seguinte forma: $a|0\rangle+b|1\rangle$, sendo a e b valores complexos. Note que o qubit expressa uma superposição linear entre duas condições pré-definidas, algo característico da mecânica quântica. Um exemplopitoresco é dado pelo experimento mental protagonizado pelo gato de Schrödinger, em que um processo de decaimento radioativo requer que se considere, antes de uma verificação de fato, o estado do felino como sendo uma combinação entre “vivo” e “morto”. É importante ressaltar que $\|a\|^2$ e $\|b\|^2$ representam probabilidade de que o sistema seja encontrado, respectivamente, dos estados $|0\rangle$ e $|1\rangle$. Uma consequência natural disso, do ponto de vista de teoria de probabilidades, é que $\|a\|^2 + \|b\|^2 = 1$. À luz dessa normalização, passa a ser muito útil representar o *qubit* tendo como pano de fundo a esfera de Bloch.



Essa casca esférica representa todos os valores válidos de $|0\rangle$ e $|1\rangle$ para um qubit, respeitando a normalização dele igual a 1.

PARALELISMO QUÂNTICO

A noção de paralelismo quântico, que permite, de certa forma, o processamento paralelo de informação, é uma propriedade responsável por uma parcela expressiva do interesse pela criação de computadores quânticos. Essa propriedade está ligada ao fato do *qubit* corresponder à superposição de diferentes estados e à perspectiva de uso de operações lineares.

O termo paralelismo quântico foi cunhado pelo físico David Deutsch [Deutsch, 1984], com intuito de diferenciá-lo do paralelismo computacional clássico, no qual dois ou mais processadores tratam dados simultaneamente. A título de exemplificação, tomemos uma função F(x) que pode ser avaliada para várias entradas numéricas. Do ponto de vista de paralelismo clássico, podemos avaliá-la para uma entrada (e.g. x=0) em um processador e para outra entrada (e.g. x=1) em outro processador; assim, obteríamos os valores para F(0) e F(1) simultaneamente. Entretanto, utilizando-se algoritmos quânticos, pode-se eventualmente realizar a avaliação da função F(x) para todos os valores de x de interesse de uma maneira organicamente paralela (decorrente da referida superposição de estados).

PORTAS LÓGICAS QUÂNTICAS

Portas lógicas quânticas, assim como portas lógicas clássicas, são dispositivos de processamento da informação fundamentais para a construção de circuitos / algoritmos. As portas, no contexto quântico, respeitam as condições de normalização e implementam operações inversíveis [Castro, 2006]. Serão exemplificadas a seguir algumas portas:

Porta de Hadamard: possui a interessante propriedade de mapear um *qubit* $|0\rangle$ou $|1\rangle$ numa sobreposição de estados:

$$|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad \text{e} \quad |1\rangle \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Porta de Pauli (X): atua sobre um *qubit* e é equivalente a uma operação de NOT:

$$|0\rangle \rightarrow |1\rangle \quad \text{e} \quad |1\rangle \rightarrow |0\rangle$$

Porta Controlled NOT (CNOT): atua sobre dois ou mais *qubits.* Para o caso de dois *qubits*, realiza uma operação similar à da porta Pauli-X no segundo *qubit* se o primeiro *qubit* for 1, e não os altera se o primeiro for 0:

$$|00\rangle \rightarrow |00\rangle,\ |01\rangle \rightarrow |01\rangle,\ |10\rangle \rightarrow |11\rangle \text{ e } |11\rangle \rightarrow |10\rangle$$

Porta de Toffoli (CCNOT): é uma porta que atua sobre três *qubits* e possui uma propriedade muito relevante: é universal do ponto de vista de implementação de qualquer função booleana. Sua atuação pode ser expressa da seguinte maneira:

$$|a, b, c\rangle \rightarrow |a, b, c \oplus ab\rangle$$

HARDWARE: ALGUMAS PONDERAÇÕES

Algumas tecnologias são apontadas como promissoras para prover meios para construção de hardware quântico: supercondutores, armadilhas de íons, quantum dots etc. Já existem até mesmo empresas no mercado que oferecem computadores de inspiração quântica – como a D Wave Systems [Dwave, 2012] – mas ainda certamente há um caminho muito vasto a ser trilhado antes de ser possível dispor dos potenciais benefícios do paradigma em escala mais ampla. Interessantemente, neste ano, ocorreu a premiação de dois físicos (Haroche e Wineland) com a máxima láurea do mundo científico – o prêmio Nobel – devido a avanços no controle preciso de estados quânticos, o que pode ter um impacto significativo na criação de hardware quântico. O futuro nessa área mostra-se promissor quando nossa visão está direcionada à disponibilidade computadores quântico em escala comercial, e, quem sabe, logo poderemos nos libertar das conjecturas e, enfim, partir à sobriedade da prática.

REFERÊNCIAS

[Feynman, 1982] R. P. Feynman, “Simulating Physics with Computers”, International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, pp. 467-488, 1982.

[Deutsch, 1984] D. Deutsch, “Quantum theory, the Church-Turing Principle and the universal quantum computer”, Proceedings of the Royal Society of London, A400, pp.97-117, 1985.

[Dwave], 2012] D Wave Systems, www.dwavesys.com. Acesso dia 22/10/2012, 11:44

[Castro, 2006] L. N. de Castro, “Fundamentals of Natural Computing: An Overview”, Physics of Life Reviews 4, pp. 25-27, 2007.