

# Computação Quântica

**Victor Valdevite Pinto, Pedro Pereira Ribeiro, Alessandro Moretti**

Instituto de Computação – Universidade Estadual de Campinas, Brazil

[victor.valdevite,pedro.pr88,alemoretti0]@gmail.com

***Abstract.** This paper aims to give a brief explanation on quantum computing and what are its benefits. First we will explain some relevant concepts of the theory of quantum mechanics applied to quantum computing. Then we will describe a quantum computer and explain some very important quantum algorithms. Finally we will go into the first quantum computer created and the prospects for the future.*

***Resumo.** Este artigo tem como objetivo fazer uma breve explanação sobre a computação quântica e quais os seus benefícios. Primeiramente iremos expor os conceitos mais relevantes da teoria da mecânica quântica aplicada à computação quântica. Em seguida iremos descrever um computador quântico e explicar alguns algoritmos quânticos muito importantes. Por fim falaremos sobre o primeiro computador quântico produzido e as perspectivas para o futuro.*

## 1. Introdução

As grandes invenções históricas dificilmente aparecem de maneira independente. A idéia de automatizar os cálculos vem desde a antigüidade e começou com a utilização de pedras e outros dispositivos que deram origem aos ábacos, progredindo durante vários séculos até o aparecimento dos computadores digitais na década de 1940 [Kowaltowski 1996].

Os computadores digitais construídos desde então seguem o modelo conhecido como Máquina de Turing, formalizado em 1936 pelo matemático inglês Alan Turing [Pozza e Penedo 2002]. O modelo proposto consiste em uma máquina de estados finitos, que opera lendo as células de uma fita horizontal infinita, uma por vez. Cada célula comporta um único símbolo, que pode ser ‘0’ ou ‘1’. A informação lida na célula em conjunto com o estado atual da máquina determina qual será o próximo estado e a ação executada: escrever, ou não, um símbolo na célula atual e mover a cabeça de leitura/escrita para a célula adjacente da esquerda ou da direita.

As arquiteturas e tecnologias se aperfeiçoaram incrivelmente desde o primeiro computador digital, aumentando a velocidade e capacidade de processamento dos novos dispositivos. Porém, assim como a tecnologia avança, os obstáculos enfrentados para expandir ainda mais suas fronteiras crescem na mesma medida. Não se espera, portanto, que a capacidade de processamento cresça indefinidamente e é provável que algoritmos que não podem ser executados em tempo hábil hoje, seguirão assim em máquinas futuras que implementem o modelo conceitual de Turing [Alves 2003].

Neste contexto, a computação quântica se posta como alternativa na qual certos problemas podem ser resolvidos de maneira muito mais rápida do que em um computador tradicional. Isso ocorre devido à propriedade conhecida como “paralelismo quântico”. Um qubit (equivalente quântico do bit) pode representar o valor lógico ‘0’, ‘1’, ou ainda os dois ao mesmo tempo. Este conceito se baseia em um princípio da mecânica quântica conhecido como *superposição coerente de estados distintos*.

Por se tratar de um tópico novo (a computação quântica tem sido levada a sério desde que Shor inventou um algoritmo quântico para fatoração de números inteiros com surpreendente ganho de performance em 1994 [Alves 2003]) ainda há grandes dificuldades na implementação física de um computador quântico. Entretanto, já se construiu hardware quântico operacional e há diversos grupos de pesquisa pelo mundo atuando nesta área.

## **2. Mecânica Quântica**

A mecânica quântica surgiu da necessidade de uma teoria que melhor descrevesse os fenômenos físicos que ocorrem nos sistemas microscópicos (a partir de  $10^{-10}$  m). Nestas escalas, os elementos não seguem os comportamentos previstos pela teoria clássica e a mecânica quântica procura explicá-los de uma maneira probabilística, pois leva em conta a natureza incerta dos estados em um sistema quântico.

Esta incerteza é descrita matematicamente como a *sobreposição de estados distintos*. A sobreposição é interpretada como a presença do sistema em mais de um estado clássico no mesmo instante. Sendo assim, o estado quântico de uma partícula é representado por um vetor em um espaço especial, conhecido como espaço de Hilbert [Alves 2003].

Outro fenômeno notável e importante para a computação quântica é a correlação. Segundo este princípio, os estados de dois elementos distintos estão ligados de tal maneira que não é possível descrever o estado de um objeto completamente sem conhecer o estado do segundo objeto [Wikipedia 2008]. Do mesmo modo, é possível conhecer informações sobre o estado de uma partícula analisando o estado de outra partícula diferente, pois as duas estão correlacionadas de alguma maneira (emaranhamento quântico).

## **3. Computadores Quânticos**

### **3.1 Bits e Qubits**

A unidade de informação do computador clássico é o bit. O bit pode ter os valores lógicos “0” ou “1”. Esses valores são representados fisicamente pela presença ou não de tensão elétrica nos componentes eletrônicos do chip. Assim, como o “0” representa a falta de tensão e o “1” a presença, os valores lógicos são mutuamente excludentes.

Analogamente, a unidade básica quântica de informação é o bit quântico ou Qubit. Um qubit pode ter os valores “0”, “1” ou qualquer superposição deles. O que substitui a tensão elétrica neste caso são quaisquer objetos quânticos que possuam dois auto estados bem distintos, tais como, os estados de polarização de um fóton, elétrons em átomos de dois níveis, spins quânticos, etc. [Oliveira 2004]

Seu estado pode ser representado por:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Para todo  $\alpha$  e  $\beta$ , números imaginários, tal que  $|\alpha|^2 + |\beta|^2 = 1$ , onde  $|\alpha|^2$  é a probabilidade do qubit estar no estado  $|0\rangle$  e  $|\beta|^2$  é a probabilidade de estar no estado  $|1\rangle$ . O estado de um qubit é então um vetor num espaço de Hilbert de duas dimensões. [Alves 2003]

É importante salientar que a definição de qubit é muito mais rigorosa e necessita de conceitos avançados de álgebra linear que estão fora do escopo deste trabalho, contudo os conceitos básicos aqui apresentados permitem entender o funcionamento de um computador quântico.

### 3.2 Registradores quânticos

Prosseguindo com a analogia, nos computadores clássicos é possível agrupar bits para formar registradores, e registrador de  $n$  bits pode assumir um único estado em determinado instante. Por sua vez, os registradores quânticos são formados de um conjunto de qubits que em determinado momento pode assumir uma superposição de  $2^n$  estados clássicos.

Um registrador quântico de 3 qubits pode ser descrito pela seguinte equação:

$$|\psi\rangle = a |000\rangle + b |001\rangle + c |010\rangle + d |011\rangle + e |100\rangle + f |101\rangle + g |110\rangle + h |111\rangle$$

E de modo geral um registrador de  $n$  qubits é descrito por  $a_i$  números imaginários, onde  $1 \leq i \leq 2^n$ , onde o quadrado da amplitude  $a_i$  representa a probabilidade que o registrador esteja naquele estado.

Assim, quando se aumenta o número de qubits, o número de bits necessários para representar cresce exponencialmente. De fato, um registrador quântico de 300 bits pode representar  $2^{300}$  bits clássicos, que é mais que todos os átomos do universo conhecido. E é neste fato que reside a grande vantagem da computação quântica, o paralelismo quântico permite avaliar uma função  $f(x)$  para muitos valores de  $x$  simultaneamente. Um computador clássico com três bits de memória, por exemplo, pode apenas armazenar três valores (uns ou zeros). Um computador quântico pode por sua vez armazenar 16 valores analógicos em pares para formar 8 números complexos. Em um dado instante temos, por exemplo:

Estado	Amplitude	Probabilidade
*	$(a+ib)$	$(a^2+b^2)$
000	$0.37 + i 0.04$	0.14
001	$0.11 + i 0.18$	0.04
010	$0.09 + i 0.31$	0.10
011	$0.30 + i 0.30$	0.18
100	$0.35 + i 0.43$	0.31
101	$0.40 + i 0.01$	0.16
110	$0.09 + i 0.12$	0.02
111	$0.15 + i 0.16$	0.05

**Tabela 1: Exemplo de superposição de estados em um registrador de 3 bits.**

A primeira coluna mostra todos os estados possíveis para os três bits. A segunda mostra a amplitude  $a_i$  de cada estado. Estes 8 números complexos são uma imagem dos conteúdos de um computador quântico num determinado momento. Durante a computação, estes 8 números irão modificar e interagir uns com os outros. Ao fim da computação um único número de 3 bits é fornecido e a terceira coluna representa a probabilidade do estado  $i$  ser o retornado. Como ao fim da avaliação da função  $f(x)$  apenas uma string de bits é fornecida, que é entendida pelo computador clássico, existe apenas uma mudança de paradigma, pois enquanto o computador clássico é determinístico, o computador quântico é probabilístico.

### 3.3 Portas Lógicas Quânticas

Os circuitos quânticos são projetados assim como os clássicos utilizando portas lógicas, exceto pelo fato que as portas lógicas quânticas devem ser reversíveis garantindo assim as propriedades matemáticas de operação de qubits, ou seja, analisando a saída é possível saber a entrada, característica que portas como AND e OR não possuem. Um exemplo de porta quântica é a operação C-NOT (não-controlado) que permite que um qubit  $a$  seja invertido se o qubit  $b$  for 1, essa operação implementa a definição de correlação, pois faz com que um bit seja dependente do outro.

Não nos prenderemos neste tópico por simplicidade mas definiremos para conhecimento que um conjunto universal de portas que permite todas as transformações é dado pelas portas C-NOT, T e Hadamart. Além disso, outras portas quânticas largamente utilizadas são: NOT quântica, Porta de Fase e Toffoli Quântica. [Mendonça 2004]

### 3.4 Medição do estado atual

Outra barreira da computação quântica é a medição do estado atual do registrador e dos bits a fim de compreender suas características, dado que a exposição à medição ou qualquer outra operação pode causar a mínima instabilidade no sistema alterando o resultado. Isso impede que algumas características sejam medidas com precisão, como a correlação. Além disso, é impossível ler o estado real do qubit para verificação, pois o resultado é probabilístico, ou seja, o que se obtém é um valor aleatório que segue as regras de probabilidade do seu estado atual. [DiVincenzo 2000]. Durante os algoritmos

os registradores quânticos são multiplicados por matrizes que tem como objetivo definir as probabilidades de cada estado, esperando-se que o resultado correto tenha a maior probabilidade após a multiplicação. O funcionamento e estrutura dessas matrizes, como já dito anteriormente, fogem do escopo do trabalho, pois necessitam principalmente de conceitos avançados de álgebra linear.

## **4. Algoritmos Quânticos**

### **4.1 Complexidade de Algoritmos**

A computação clássica permite que vários problemas sejam resolvidos de forma eficiente em tempo polinomial no tamanho da entrada no pior caso, como por exemplo, criação de árvore geradora em grafos, ordenação de vetores, multiplicação de matrizes, etc. Esses problemas estão na classe P. Por outro lado existem problemas que até hoje não se sabe se podem ser resolvidos em tempo polinomial, crescendo exponencialmente com a entrada. Estes problemas estão na classe NP, que comporta também os NP-Completo, que é uma subclasse que contém os NP mais difíceis. Neste conjunto estão o problema do 3-SAT, Caixeiro Viajante, Vertex Cover, entre tantos outros. Por fim existem os que não podem ser resolvidos, são eles os problemas indecidíveis, neste seletto conjunto disjuncto de qualquer outro, está o problema da parada.

Existem outras classes de problemas importantes como o BPP ( $P \subseteq BPP$ ) - Bounded-error probabilistic polynomial time - que contém os problemas que podem ser resolvidos em tempo polinomial utilizando uma Máquina de Turing probabilística, diferente da Máquina de Turing clássica que é determinística, onde um conjunto de números aleatórios gerados permite a resolução com uma pequena probabilidade de erro.

Com o advento da computação quântica, surgiram algoritmos quânticos que se suspeita não respeitar o teorema de Church-Turing. Este teorema impõe que qualquer implementação de modelos computacionais pode ser simulada por uma Máquina de Turing probabilística. Entretanto, é provável que esta não consiga simular uma máquina quântica. Com isso surgiram novas classes de problemas que visam ampliar a teoria da complexidade computacional inserindo nesse contexto modelos computacionais quânticos.

Uma destas classes é análoga ao BPP e é conhecida como BPQ (Bounded-error quantum polynomial time). Ela contém problemas que podem ser resolvidos de forma eficiente por máquinas quânticas com uma pequena probabilidade de erro. E é devido à solução de problemas desta classe o motivo de grande parte do interesse em computação quântica. O algoritmo de Shor, por exemplo, resolve um desses problemas permitindo a fatoração de números grandes de modo incrivelmente eficiente. Isto afeta seriamente a segurança dos sistemas criptografados baseados em chave pública, tornando-os vulneráveis a uma possível quebra com o uso deste algoritmo.

A computação quântica também foi impulsionada pela descoberta do algoritmo de Grover que permite a procura de dados não ordenados em base de dados. Assim mais um problema de grande importância prática que era inviável computadores clássicos, principalmente em bases muito grandes, pode ser resolvido em tempo viável e com maior eficiência. [Marquezan 2004]

Em termos de ganho de complexidade em relação aos clássicos podemos dividir os algoritmos quânticos em dois tipos, os da classe A são exponencialmente mais rápidos e os da classe B que são quadraticamente mais rápidos. O algoritmo de Grover se enquadra na classe B e o de Shor está na classe A. Existem algoritmos que não estão em nenhuma das duas classes como o de Deutsch, pois ele não tem análogo clássico. [Oliveira 2004]

É importante ressaltar neste tópico que diferentemente da crença geral, há fortes indícios que os problemas da classe NP não poderão ser solucionados pelas máquinas quânticas.

Vamos agora estudar alguns desses algoritmos quânticos e verificar os ganhos de complexidade destes.

#### **4.2 Algoritmo de Shor**

O problema de achar os fatores primos de um número composto  $N$  tinha no General Number Field Sieve (GNFS) seu algoritmo mais eficiente com complexidade  $O(e^{1/3 \cdot \log(n^{2/3})})$ , para se ter uma idéia para um número de 1024 bits são necessários aproximadamente 100 mil anos em computador comum para se obter os fatores primos. Em 1994, Peter Shor mostrou que era possível resolver eficientemente esse problema usando a computação quântica. Em fato o algoritmo de Shor encontra os fatores em complexidade  $O(n^2 \cdot \log n \cdot \log \log n)$  utilizando para isso a transformada de Fourier quântica. [Shor 1994]

A idéia básica por trás do algoritmo de Shor é que para a fatoração de dado número  $n$  é preciso encontrar, dado um número inteiro  $x$ , o menor inteiro  $r$  tal que

$$x^r = 1 \pmod{n}$$

Isso equivale a calcular o período de uma função exponencial modular. A Figura 1 apresenta uma parte do algoritmo de Shor, um maior detalhamento do funcionamento do algoritmo pode ser encontrado em [Wallace 2004].

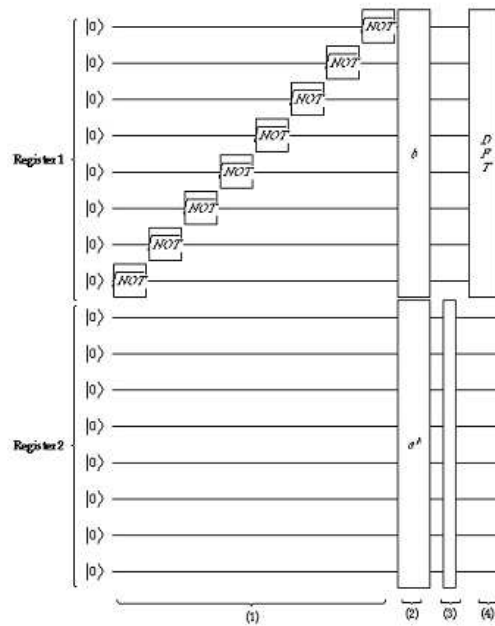


Figura 1: Algoritmo de Shor

O algoritmo de Shor provou, portanto, que os computadores quânticos podem trazer ganhos até exponenciais em tempo de execução para problemas que não tem solução eficiente sob o ponto de vista da computação clássica. E com isso, em teoria, este algoritmo quebra muito dos sistemas criptográficos utilizados atualmente e assim os sistemas atuais não são seguros. Haverá a necessidade de uma recriptografia das chaves usando números maiores ainda, que possuam mais bits do que os qubits dos computadores quânticos mais poderosos. Outra solução são os novos investimentos em criptografia quântica, uma vez que para valores de qubits na casa das centenas se torna impraticável aumentar o número de bits de modo que os números sejam maiores que o que os qubits podem representar.

### 4.3 Algoritmo de Grover

Outro problema que tem sua complexidade melhorada é o de encontrar um elemento específico em uma lista não ordenada com  $N$  elementos. No computador clássico temos que testar elemento por elemento, no pior caso possível precisamos realizar  $N$  testes. Usando as bases da mecânica quântica o Algoritmo de Grover [Grover 1996] permite que a quantidade de testes necessários seja proporcional a  $\sqrt{N}$ , o que o coloca como um algoritmo de classe B. O algoritmo consiste em realizar buscas nos índices dos elementos ao invés de buscar os próprios elementos, assim utilizando dois registradores quânticos é necessário avaliar a quantidade de vezes que a função

$$f : \{0, 1, \dots, N - 1\} \rightarrow \{0, 1\},$$

definada por

$$f(i) = \begin{cases} 1, & \text{se } i = i_0, \\ 0, & \text{se } i \neq i_0, \end{cases}$$

é invocada. Para isso imaginamos que  $f$  é uma função que está a disposição para adivinhar, como um oráculo, se um elemento é ou não o procurado. Mais informações sobre o funcionamento desse algoritmo em [Portugal 2005]

#### 4.4 Outros Algoritmos

##### 4.4.1 Algoritmo de Deutsch

Esse algoritmo permite verificar se uma função binária é constante ( $f(0) = f(1)$ ) ou equilibrada ( $f(0) \neq f(1)$ ), realizando apenas uma operação com a função. Seria como se pudesse saber se uma moeda possui de um lado cara e do outro coroa com apenas uma observação. [Oliveira 2004]

##### 4.4.2 Algoritmo de Simon

Por fim temos o algoritmo de Simon que consiste em encontrar um  $c$  dada uma função  $f: F_2^n \rightarrow F_2^n$  dois para um, ou seja, a cada par de valores distintos no domínio corresponde a uma única imagem no contradomínio, isto é:

$$f(x) = f(y) \Leftrightarrow x \equiv y + c \pmod{F_2^n}$$

A complexidade clássica é de  $O(2^{n/2})$  enquanto o algoritmo quântico tem complexidade  $O(n^2 + nF)$  onde  $F$  é o custo de calcular  $f$ . [Shor 2002]

## 5. Computador Orion

Em fevereiro de 2007 a empresa D-Wave apresentou ao mundo o primeiro computador quântico em funcionamento. Chamado Orion (figura 2), este computador surpreendeu muitos cientistas que apostavam que o primeiro computador dessa linha seria apresentado somente em 20 anos.

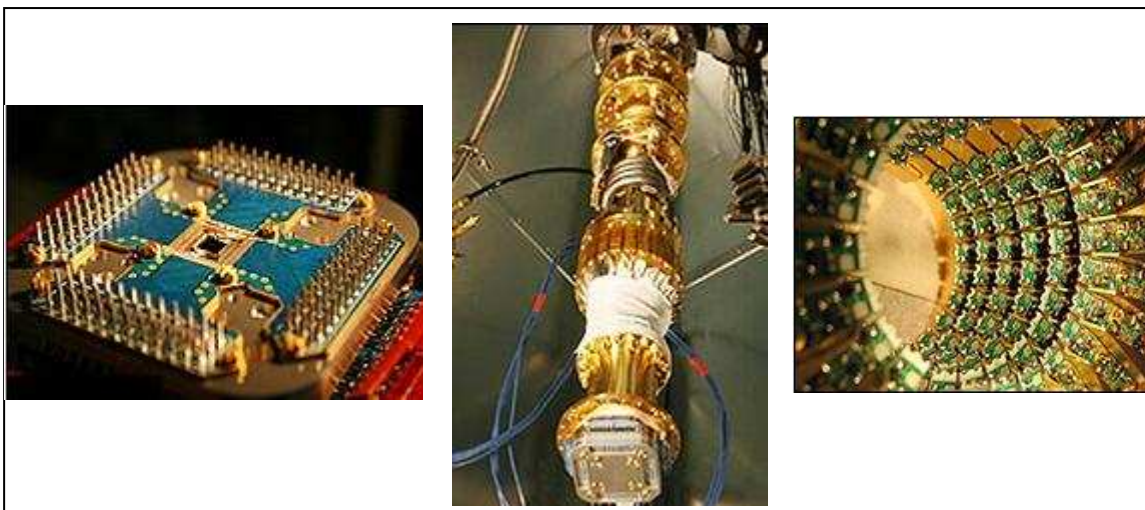


Figura 2: Imagens do Orion

Após a apresentação deste computador pela D-Wave na SC07 supercomputing conference em Reno, Nev., Hartmut Neven [D-Wave 2007] muitos cientistas ficaram receosos, pois acham que o Orion é mais um computador convencional com algumas peculiaridades de computação quântica porque a empresa responsável não expôs as

especificações técnicas do computador, tentando proteger seu projeto de 44 milhões de dólares.

Com um sistema híbrido (digital e quântico) e 16 qubits, o Orion resolveu problemas de lógica, soluções para o jogo Sudoku e pesquisou alternativas para drogas usadas na indústria farmacêutica. Todas essas tarefas poderiam ser executadas por um computador convencional, mas a demonstração confirma as expectativas de que o modelo de computação quântica pode ser realmente utilizado na prática.

Dentre as muitas possibilidades de fabricação de um computador quântico, o Orion foi fabricado em um único chip quântico. Sobre uma base de silício, esse chip abriga os 16 qubits, que seriam equivalentes a 65536 bits de um computador convencional. Cada um deles é formado por uma porção de nióbio circundada por uma bobina. Quando a bobina é estimulada eletricamente, ela gera um campo magnético, que provoca alterações de estado nos átomos de nióbio. Essas mudanças de estado são captadas pelos circuitos e transformadas em dados.

Para que o Orion possa processar informações, elas primeiro são convertidas em impulsos analógicos, que são enviados às bobinas. Depois, os sinais analógicos coletados são novamente convertidos em bits. Como os sinais analógicos podem sofrer interferências, um complexo filtro de 128 canais é usado para eliminar o ruído. Assim, o processador quântico pode interagir com circuitos digitais convencionais [Maurício Grego 2007]. Para que tudo isso funcione, é necessário congelar o chip a 4 mK (milikelvins), pois o nióbio se torna supercondutor a essa temperatura. Um dos grandes problemas para se construir um computador quântico era justamente a temperatura e, o Orion, é congelado nesta temperatura utilizando um sistema de refrigeração com hélio líquido.

Mesmo sendo um computador com sistema híbrido, o Orion já provou que há possibilidade de construir um computador seguindo os padrões quânticos. Assim há possibilidade de que alguns dos grandes problemas em computação sejam resolvidos através dos algoritmos quânticos e do computador quântico.

#### **4. Perspectivas futuras e Conclusões**

Após a apresentação do primeiro computador quântico já produzido muitos acreditavam que seria muito difícil aprimorar rapidamente esse modelo, pois a empresa que criou o Orion não divulgou muitos detalhes técnicos, dificultando o progresso científico nessa área. Mesmo com esse cenário de desconfiança, a mesma empresa, D-Wave, apresentou em novembro de 2007 outro computador quântico no mesmo conceito de Orion, porém agora com 28 qubits. Com um alto investimento em computação quântica, a empresa promete apresentar um computador quântico de 1024 qubits no fim de 2009, que chamará "Monte Carlo". O Monte Carlo será totalmente quântico, não terá interface com qualquer computador digital e estará disponível para pesquisas online [D-Wave 2007], segundo a empresa D-Wave.

## Referências

- Kowaltowski, T. (1996) “Von Neumann: suas contribuições à Computação”. Em: *Estudos Avançados*, USP, 10, 26, 1996, pp. 237-270.
- Pozza, O. e Penedo, S. (2002) “A Máquina de Turing”, Universidade Federal de Santa Catarina, Brasil. <http://www.inf.ufsc.br/~barreto/trabaluno/MaqT01.pdf>
- Alves F. (2003) “Computação Quântica: Fundamentos Físicos e Perspectivas”. Universidade Federal de Lavras, Brasil.
- DiVincenzo F. P. (2000), “The Physical Implementation of Quantum Computation”, IBM
- de Mendonça P. E. M. F. (2004), “Estudo de Portas Lógicas Quânticas de Dois Qubits Definidas em um Subespaço Livre de Decoerência para um Sistema de Quatro Qubits Acoplado ao Resto do Universo por um Agente Degenerado”, Universidade de São Paulo, São Carlos, SP
- Marquezan C. C. (2004), “Computação Quântica: Algoritmos e Simuladores”, Universidade Federal do Rio Grande do Sul, Porto Alegre, RS
- Shor P. (1996), “Polynomial-Time Algorithms for Prime Factorisation and Discrete Logarithms on a Quantum Computer”
- Shor P. (2002), “Introduction to Quantum Algorithms”, In: *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, Edited by: Samuel J. Lomonaco Jr.
- Oliveira I. S. e Sarthour R. S. (2004), “Computação Quântica e Informação Quântica”, Centro Brasileiro de Pesquisas Físicas
- Portugal, R. (2005), “Uma Introdução à Computação Quântica”, Vitória, ES
- Knuth, D. E. (1984), *The TeXbook*, Addison Wesley, 15<sup>th</sup> edition.
- Smith, A. and Jones, B. (1999). On the complexity of computing. In *Advances in Computer Science*, pages 555–566. Publishing Press.
- Grego, M. (2007) “Computador Quântico já funciona”, Info Online, Brasil. <http://info.abril.com.br/aberto/infonews/022007/15022007-3.shl>
- D-Wave Systems (2007) “D-Wave Systems News”, D-Wave Systems, Inglaterra. <http://www.dwavesys.com/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=4&cntnt01returnid=21>
- D-Wave Systems (2007) “D-Wave Systems News”, D-Wave Systems, Inglaterra. <http://www.dwavesys.com/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=9&cntnt01origid=15&cntnt01returnid=21>