Introdução à Computação Quântica

Hamilton José Brumatto - RA 096389
Universidade Estadual de Campinas
brumatto@ic.unicamp.br

RESUMO

A evolução dos computadores está limitada por duas barreiras inatingíveis para o modelo atual: velocidade da luz no processamento da informação e a dimensão da ordem de grandeza atômica, no tamanho dos componentes em um chip. A Computação Quântica é a continuidade natural na evolução dos computadores para fisicamente tentar atingir estas barreiras. O princípio da incerteza associado à estrutura quântica da matéria define um mecanismo para que Computadores Quânticos implementem uma Máquina Probabilística de Turing, assim os Computadores Quânticos poderão ser utilizados na solução de problemas intratáveis da classe NP-completo. É possível definir Bits Quânticos, ou Qubits, para representação da informação e construir um conjunto universal de portas quânticas para operar sobre os Qubits, seguindo uma programação pré-definida. Alguns protótipos já demonstram a implementação da computação quântica, no entanto são apenas modelos experimentais. A Computação Quântica apresenta uma perspectiva positiva de futuro.

Categories and Subject Descriptors

B.2.0 [**Hardware**]: Arithmetic and Logic Structure - general—*Quantum Computing*

General Terms

Theory

Keywords

Computação Quântica, Qubit, Porta Lógica Quântica

1. INTRODUÇÃO

A Lei de Moore[10] traz uma predição que tem se confirmado nos últimos anos[5], no entanto não é possível que a taxa de crescimento predita ou medida se mantenha, e isto é evidenciado por uma quebra mais recente no ritmo do crescimento[5]. Um dos motivos da dificuldade de manter o crescimento é que o aumento do número de componentes em um chip implica na diminuição do tamanho de cada componente, neste caso, se a taxa de crescimento se mantiver teremos componentes atingindo o tamanho de um átomo, o que é uma situação impossível. Outro fator a se considerar é o limite na solução de problemas computacionais que a arquitetura concebida no modelo da Máquina de Turing oferece, por mais rápido que sejam as máquinas ainda não é possível resolver problemas considerados NP-completos[2] para uma entrada suficientemente grande. Conclui-se então que há a necessidade de se criar um novo paradigma na construção de hardware.

Uma máquina probabilística de Turing[2] é suficiente para resolver problemas definidos NP-completos, em tempo polinomial. Com base nesta idéia, David Deutsch procurou definir um dispositivo computacional capaz de simular eficientemente sistemas físicos arbitrários[12] como base para a construção de uma máquina probabilística. Como os sistemas físicos são basicamente ditados pela mecânica quântica, surgiu a proposta inicial de construção de computadores quânticos, esta idéia se desenvolveu até a concepção moderna da computação quântica.

A base da computação quântica é a representação de um bit, o *Qubit*. É necessário um sistema quântico que apresente dois estados bem definidos, indicados por $|\mathbf{0}>$ e $|\mathbf{1}>$. Apesar de possuir estes dois estados quânticos fundamentais, o sistema utilizado poderá se encontrar em um estado que é na realidade uma sobreposição dos estados fundamentais. A sobreposição é indicada por uma distribuição probabilística através dos estados fundamentais. O estado do sistema fica descrito por um vetor, cada posição do vetor está associada a um estado fundamental e o valor representado define a probabilidade do Qubit estar naquele estado fundamental. Em um sistema com n Qubits teremos 2^n estados fundamentais possíveis. Ao medir o sistema obtemos um único valor que indica apenas o conjnto de estados fundamentais nos quais cada Qubit do sistema se encontra, o estado medido segue à distribuição probabilística. Este mecanismo é a base de concepção de uma máquina probabilística de Turing.

Uma arquitetura proposta é construída de forma semelhante à arquitetura clássica: Memória, ULA e Circuito de Controle. Memória e ULA são dispositivos quânticos, o Circuito de controle possui uma interface na computação clássica para gerenciar o controle de fluxo quântico e mecanismos de correção de erro. A ULA é construída através de um conjunto universal de *portas lógicas* quânticas. Algumas

propriedades físicas têm sido exploradas para implementar uma máquina real, no entanto os protótipos ainda trabalham com cerca de uma dezena de Qubits, o que é ainda insuficiente para qualquer resultado prático.

2. INCERTEZA POR PRINCÍPIO

A física clássica é fundamentada pela descrição dos movimentos dos corpos introduzida por Sir Isaac Newton[11], e também pela descrição do comportamento dos campos e ondas eletromagnéticas compilada por James Clerk Maxwell[9]. As várias teorias, teoremas e experimentos construídos ao longo dos últimos séculos pelos sucessores e até mesmo antecessores de Newton e Maxwell demonstraram que as equações da mecânica e do eletromagnetismo descrevem com grande sucesso os fatos observados. No início do século passado, alguns experimentos ficavam inexplicados: por exemplo, pela teoria do eletromagnetismos, um elétron quando acelerado emite energia na forma de radiação eletromagnética e com isto, baseado no princípio da conservação da energia, diminui sua própria energia de movimento, decorrente disto um elétron submetido à ação de uma força (aceleração) centrípeta em um movimento ao redor do núcleo deve perder sua energia e se precipitar no núcleo, o que não ocorre.

Outras contradições entre fatos reais/experimentais e previsões teóricas surgiram, entre eles um famoso problema, a catástrofe do ultravioleta de Rayleigh e Jeans[1]. O problema considera que um corpo negro teria uma energia infinita, a energia é função da temperatura e da freqüência da radiação eletromagética. Dada uma freqüência, a energia obtida é uma integral em um intervalo contínuo e isto faz com que esta integral resulte em valor infinito quando calculada para freqüências na região do ultravioleta. Max Planck resolveu este problema, ele propôs que a energia não assuma valores contínuos, e sim múltiplos de um valor mínimo: $E = nh\nu$, sendo ν a freqüéncia, h uma constante (constante de Planck) e n valores inteiros, o valor mínimo possível, $E = h\nu$ é o *Quanta* de energia. Com isto a energia total passou a ser uma soma discreta e não mais uma integral, coerente com os resultados experimentais. Com a definição do *Quanta* de energia, os valores de energia possíveis são "quânticos". Este foi o primeiro trabalho que deu início à Física Quântica.

Heisenberg[4] em seu trabalho sobre princípios da teoria quântica, trouxe uma compilação de vários experimentos que apresentava a ambiguidade entre a natureza corpuscular e ondulatória da matéria. Por exemplo, raios β ao passarem por uma câmara de bolhas deixam um rastro compatível com a natureza de uma partícula, é possível determinar massa e velocidade. Por outro lado, os raios β ao atravessarem um filme fino de material cristalino formam uma figura de difração em um anteparo, compatível com a natureza de uma onda, é possível medir sua freqüência. Isto significa que um feixe de raios β pode ser descrito tanto como uma frente de onda quanto como um conjunto de partículas. O mesmo foi observado para os raios X, que como são radiações eletromagnéticas, possuem a natureza de onda. Quando um feixe deste raio atravessa um vapor supersaturado de água, é deixado um rastro tal qual um conjunto de partículas, também se observa o efeito de difração para o raio X. Decorrente da natureza dual partícula-onda Heisenberg deduziu que o conhecimento da posição de uma partícula com a precisão Δx e o conhecimento do momento (velocidade) da partícula com a precisão Δp deve obedecer o limite: $\Delta x \cdot \Delta p \geqslant \frac{h}{4\pi}$, sendo h a constante de Planck. Este resultado é conhecido como o *Princípio de Incerteza* de Heisenberg, e deriva diretamente da dualidade partícula-onda, não é possível conhecer simultaneamente a posição e velocidade de uma partícula, exceto dentro de um limite de incerteza, que é pequeno comparado ao valor da massa de corpos do nosso cotidiano, mas é expressivo em um mundo subatômico.

Enquanto realizava experiências para evidenciar a dualidade partícula-onda também para a luz que é uma forma de radiação eletro-magnética, Eisntein demonstrou através do efeito foto-elétrico, o que lhe valeu um prêmio Nobel, que a luz também pode ser interpretada na forma de partícula, chamada fóton. Com base nisso propôs-se uma experiência na obtenção de figuras de difração a partir de fótons[15]. Nesta experiência emite-se luz com intensidade bem baixa, quase que um fóton por vez, de forma a passar por um anteparo com dois furos, observa-se que no resultado cada fóton imprime uma imagem que compões ao longo do tempo, com a imagem de outros fótons, a figura da difração, isto indica que a natureza onda do fóton permite que este, mesmo sendo uma única partícula, atravesse ao mesmo tempo ambos furos formando a figura de difração, e cada fóton acaba sendo impresso como um ponto, ou partícula, no anteparo. Se for colocado um tipo de detecção, logo na saída dos furos para identificar por qual furo o fóton passa, de fato, observa-se que cada fóton passa por um único furo, no entanto perde-se a figura de difração. A medida da posição ou velocidade do fóton afeta seu estado.

O princípio da incerteza e o resultado de que uma medida afeta o estado de uma partícula nos limites quânticos nos permitirá entender o modelo da computação quântica.

3. 0 OU 1 OU ... TALVEZ

O conceito dos Bits Quânticos[3] leva em consideração estados quânticos da matéria. Um bit pode ser representado por um sistema quântico que possua dois estados fundamentais, que podem ser indicados como estados booleanos $|\mathbf{0}>$ e $|\mathbf{1}>$[1]. Os estados quânticos são ortogonais, portanto podem representar estados booleanos, ou seja:

$$<\mathbf{0}|\mathbf{0}>=1, <\mathbf{1}|\mathbf{0}>=0, <\mathbf{0}|\mathbf{1}>=0 \text{ e } <\mathbf{1}|\mathbf{1}>=1 \quad (3.1)$$

Se um sistema for medido no estado representado como $|\mathbf{0}>$, então não está no estado $|\mathbf{1}>$. No entanto, como visto na seção anterior, os estados quânticos que um sistema pode apresentar não recai necessariamente em um ou outro estado fundamental, o princípio de incerteza nos diz que há uma probabilidade de o sistema simultaneamente estar em um ou outro estado fundamental, um determinado estado ψ pode ser representado de acordo com esta probabilidade como:

$$|\psi>=\alpha|\mathbf{0}>+\beta|\mathbf{1}> \quad (3.2)$$

Como os estados são ortogonais, devemos ter $\alpha^2+\beta^2=1$, α^2 e β^2 representam a probabilidade do sistema estar em um ou outro estado. Um conceito mais geral deve considerar estas constantes como números complexos, não vamos nos preocupar com isto agora.

[1]A notação apresentada é a notação *bra-ket*[13] definida por Paul Dirac para representação de estados quânticos.

Para entender melhor, vamos considerar o sistema *Átomo de Hidrogênio*, neste átomo o único elétron fica na camada s da eletrosfera. Segundo o princípio de exclusão de Pauli[8], na camada s da eletrosfera é possível coexistir dois elétrons desde que possuam spins distintos, spin *Up* e spin *Down*, são estados distintos. Cada estado apresenta um nível diferente de energia. Portanto, no átomo de hidrogênio o único elétron pode estar em um ou outro estado dado o princípio da incerteza, a representação possível é uma função de probabilidade que distribui o elétron sobre um ou outro estado. Este conceito pode se expandir a sistemas que apresentem vários estados fundamentais, o sistema poderá estar em uma distribuição probabilística sobre os estados, se forem quatro estados, poderão representar dois Qubits simultãneos em seus estados fundamentais.

Ao trabalhar com sistemas que possuam dois Qubits, um Qubit estará no estado ψ e o outro no estado ϕ, cada qual representado por uma distribuição

$$\begin{array}{c} |\psi>=\alpha|\mathbf{0}>+\beta|\mathbf{1}> \text{ e} \\ |\phi>=\eta|\mathbf{0}>+\delta|\mathbf{1}> \end{array} \tag{3.3}$$

com isso teremos no final uma sobreposição probabilística dos vários estados fundamentais representando o estado do sistema quântico:

$$\begin{aligned} |\psi>\otimes|\phi> &= |\psi>|\phi> \\ &= (\alpha|\mathbf{0}>+\beta|\mathbf{1}>)\otimes(\eta|\mathbf{0}>+\delta|\mathbf{1}>) \\ &= \alpha\eta\left(|\mathbf{0}>\otimes|\mathbf{0}>\right)+\alpha\delta\left(|\mathbf{0}>\otimes|\mathbf{1}>\right) \\ &\quad +\beta\eta\left(|\mathbf{1}>\otimes|\mathbf{0}>\right)+\beta\delta\left(|\mathbf{1}>\otimes|\mathbf{1}>\right) \\ &= \alpha\eta|\mathbf{00}>+\alpha\delta|\mathbf{01}>+\beta\eta|\mathbf{10}>+\beta\delta|\mathbf{11}> \\ &= \alpha\eta|\mathbf{1}>+\alpha\delta|\mathbf{2}>+\beta\eta|\mathbf{3}>+\beta\delta|\mathbf{4}> \end{aligned} \tag{3.4}$$

A última linha da equação acima apresenta uma notação mais simples para os estados fundamentais em sistemas com dois Qubits. Fica claro que um sistema que apesenta quatro estados fundamentais pode representar um sistema com dois Qubits. Outro detalhe na equação acima é a linearidade, isto é possível, pois os estados são bem descritos por um vetor, ou seja, os estados $|\mathbf{0}>$ e $|\mathbf{1}>$ são ambos auto-vetores que representam soluções possíveis para um estado quântico:

$$\alpha|\mathbf{0}>+\beta|\mathbf{1}>=\alpha\begin{bmatrix}1\\0\end{bmatrix}+\beta\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix} \tag{3.5}$$

Podemos representar, desta forma:

$$|\psi>\otimes|\phi>=\begin{bmatrix}\alpha\\\beta\end{bmatrix}\otimes\begin{bmatrix}\eta\\\delta\end{bmatrix}=\begin{bmatrix}\alpha\eta\\\alpha\delta\\\beta\eta\\\beta\delta\end{bmatrix} \tag{3.6}$$

Dada a lineridade, quando realizamos uma medida no sistema acima em apenas um Qubit, o Qubit seguinte pode se apresentar em qualquer outro estado. Feita a medida, e supondo que o primeiro bit se encontra no estado m, $m \in \{0,1\}$, o estado resultante é:

$$|\mathbf{\Psi}>=\eta|\mathbf{m},\mathbf{0}>+\delta|\mathbf{m},\mathbf{1}> \tag{3.7}$$

Porém nem todos os estados podem ser descritos por uma combinação linear de dois estados separados, considere o estado representado pela equação (3.8), uma vez feita a leitura do primeiro bit, no estado m, o segundo bit, necessariamente, estará no mesmo estado m. Este estado é conhecido como *Estado de Bell*, este estado não é atingível por uma combinação linear de estados individuais dos Qubits. O Estado de Bell ou par EPR (Einstein, Podolsky e Rosen) apresenta correlações fortes, maiores que quaisquer outras que poderiam existir em sistemas clássicos[12]. Este estado é a chave para o teleporte-quântico que falaremos nas mais à frente.

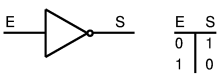

Figura 1: Porta *NÃO* da lógica binária

$$|\mathbf{\Psi}>=\eta|\mathbf{0},\mathbf{0}>+\delta|\mathbf{1},\mathbf{1}> \tag{3.8}$$

Se considerarmos um sistema com n Qubits, teremos um estado final $\mathbf{\Psi}$ que é a junção dos vários estados individuais ψ_i, conforme vemos na equação abaixo, além dos Estados de Bell para o sistema de múltiplos Qubits. Os estados possíveis do sistema crescem, assim, de forma exponencial. As operações em um computador quântico ocorrem através de portas quânticas sobre estados quânticos do sistema, as medidas são obtidas com base na distribuição probabilística na descrição do estado. A partir do momento que temos um conjunto de medidas sobre a distribuição probabilística nos estadosdo sistema podemos intuir que um computador baseado em sistemas quânticos representa uma implementação da Máquina Probabilística de Turing[13].

$$|\mathbf{\Psi}>=|\psi_1>\otimes|\psi_2>\otimes|\psi_3>\otimes\ldots\otimes|\psi_n> \tag{3.9}$$

4. TODAS AS PORTAS: NÃO

Tal qual na computação clássica, as portas "*lógicas*" devem operar sobre *bits* de entrada gerando *bits* na saída, a diferença é que na computação quântica as portas devem operar sobre estados quânticos. Podemos definir uma porta lógica quântica como um dispositivo que consegue realizar, em um período finito de tempo, uma operação unitária definida em um conjunto específico de Qubits[3].

4.1 Portas de 1 Qubit

A única porta da lógica binária clássica não trivial de 1 bit é a porta *NÃO*, a figura 1 apresenta um diagrama para a porta *NÃO* incluindo a tabela verdade que indica a saída conforme a entrada.

O que esperamos para uma porta *NÃO* quântica é a capacidade de, dado um estado quântico fundamental como entrada, resultar no estado quântico inverso. Se esta porta operar sobre o estado $|\mathbf{0}>$ devemos obter como saída o estado $|\mathbf{1}>$ e também o inverso. Como os estados quânticos são representados por uma notação vetorial. Os operadores que modificam estes estados são representados por matrizes. A porta NÃO quântica, chamada de Porta X (troca o bit quântico) está representada na figura 2, quando aplicada sobre o estado $|\mathbf{0}>$ resulta no estado $|\mathbf{1}>$ e vice-versa. O uso da porta X pode ser visto na equação 4.1

$$\begin{aligned} X|\mathbf{0}>=|\mathbf{1}> \quad &\text{e} \quad X|\mathbf{1}>=|\mathbf{0}> \\ X\left(\alpha|\mathbf{0}>+\beta|\mathbf{1}>\right) &= \alpha X|\mathbf{0}>+\beta X|\mathbf{1}> \\ &= \alpha|\mathbf{1}>+\beta|\mathbf{0}> \\ X\begin{bmatrix}\alpha\\\beta\end{bmatrix} &= \begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix}=\begin{bmatrix}\beta\\\alpha\end{bmatrix} \end{aligned} \tag{4.1}$$

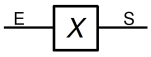

Figura 2: Porta *X* quântica

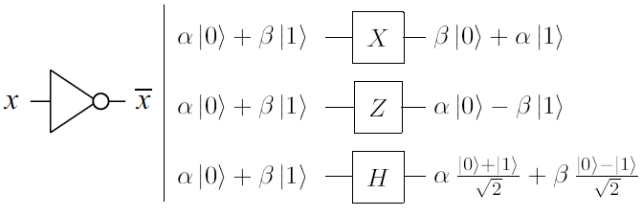

Figura 3: Portas de 1 bit clássica (esq) e quântica (dir)[12]

Aplicar uma porta sobre um Qubit é o mesmo que utilizar uma matriz 2×2. Uma porta quantica deve ser unitária, Dada uma porta U qualquer, para que ela seja unitária, a seguinte relação deve ser válida:

$$U^\dagger U = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4.2}$$

Na equação acima, $U^\dagger$ é o adjunto do operador U, ou seja, é o operador definido pela matriz transposta e conjugada. É fácil ver que $X^\dagger X = I$. O mais curioso é que só existe esta restrição para construção de portas quânticas. Para o Qubit podemos definir outras, portas além da porta X, temos por exemplo a Porta Z:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{4.3}$$

A porta Z não altera o estado $|\mathbf{0}>$, mas muda o sinal do estado $|\mathbf{1}>$ para $-|\mathbf{1}>$. Outra porta muito utilizada é a porta H, a porta de *Hadamard*, ela é conhecida como "raiz quadrada de NÃO":

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{4.4}$$

A porta não é de fato a raiz quadrada de NÃO, pois $H^2 = I$, ou seja, aplicar H duas vezes não irá alterar o estado de um Qubit. H aplicada em $|\mathbf{0}>$ transforma em $(|\mathbf{0}> + |\mathbf{1}>)/\sqrt{2}$ e aplicada em $|\mathbf{1}>$ transforma em $(|\mathbf{0}> - |\mathbf{1}>)/\sqrt{2}$ ambos são estados que estão no meio do caminho de $|\mathbf{0}>$ e $|\mathbf{1}>$. Por isso é chamada de raiz quadrada, ela faz uma meia troca de bit, podemos interpretar como um deslocamanto de fase. A figura 3 apresenta uma comparação entre as portas lógicas quânticas e a porta lógica binária clássica.

As portas X e Z são portas chamadas *Pauli-X* e *Pauli-Z*, e estas compõem com a porta Y (*Pauli-Y*) as portas de inversão. As portas S (*Fase*) e T ($\pi/8$) completam, com a porta H, as portas de deslocamento de fase, não podemos nos esquecer que os estados quânticos podem ser representados por números complexos. Podemos interpretar os índices de probabilidade na distribuição sobre os estados fundamentais como representação de fase na superfície de uma esfera de raio um, as operações aplicadas através das portas quânticas são apenas operações de rotações nesta superfície, algumas portas indicam inversão (*flip*), e outras portas rotações de

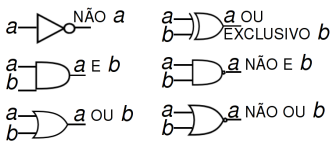

Figura 4: Portas de 2 bits da lógica clássica

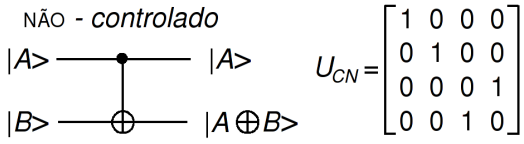

Figura 5: Porta *C-NOT* de 2 Qubits da lógica quântica

um eixo para outro, existem portas que oferecem uma rotação de fase menor que $\pi/2$. A porta de Fase S é considerada a raiz quadrada da porta Z de Pauli e a porta $\pi/8$ é a raiz quadrada da porta de Fase, tal qual a porta Hadamard é a raiz quadrada da porta X.

$$\begin{aligned} Pauli - Y &: Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ Fase &: S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\ \frac{\pi}{8} &: T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \end{aligned} \tag{4.5}$$

Na realidade podem existir infinitas portas para um único Qubit, no entanto, como as portas são unitárias, qualquer porta pode ser representada por um conjunto de rotações no campo complexo.

4.2 Portas de N Qubits e Operações Quânticas

Se um sistema quântico possui múltiplos Qubits, esperamos que as portas lógicas interajam com todos Qubits não apenas como operações isoladas em cada bit. Podemos fazer uma comparação com o modelo de dois bits clássicos, onde definimos um conjunto de portas que podem ser vista na figura 4. Dentre estas, as portas *NÃO* e *NÃO E* são consideradas universais, pois a partir destas duas é possível construir quaisquer outras portas.

Algo smelhante se aplica à computação quântica. Na lógica clássica, uma porta E possui duas entradas e fornece uma única saída, na lógica quântica, como os estados são representados por vetores de dimensão 2^n (n é a quantidade de Qubits) e os operadores são representados por matrizes de tamanho $2^n \times 2^n$ então a saída será o mesmo número de entradas. A figura 5 exibe a porta *NÃO - controlada* ou *C-NOT* sobre dois Qubits. A representação gráfica indica duas linhas de entrada representando cada Qubit, a porta é representada como barra vertical com símbolos característicos nas extremidades, o círculo fechado representa o bit de controle da porta. Na mesma figura está a representação matricial da porta.

A porta *C-NOT* atua realizando a operação da porta X no

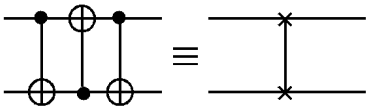

Figura 6: Porta *Troca* construída a partir de portas *C-NOT*

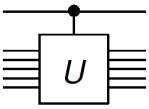

Figura 7: Porta *U-Controlada* para n Qubits

segundo Qubit somente se o primeiro (Qubit de controle) estiver no estado $|\mathbf{1}>$, caso contrário não realiza qualquer alteração. Ou seja, a tabela 1 abaixo indica entradas e saídas da porta *C-NOT*.

$$|\mathbf{00}> \mapsto |\mathbf{00}>$$
$$|\mathbf{01}> \mapsto |\mathbf{01}>$$
$$|\mathbf{10}> \mapsto |\mathbf{11}>$$
$$|\mathbf{11}> \mapsto |\mathbf{10}>$$

Tabela 1: Operador *C-NOT* aplicado aos estados fundamentais de um sistema de 2 Qubits

A porta *C-NOT* pode ser interpretada também através do uso da operação *OU - Exclusivo* "$\oplus$" como está representado na figura 5, $U_{CN}|\mathbf{A},\mathbf{B}> \mapsto |\mathbf{A},\mathbf{A}\oplus\mathbf{B}>$, ou seja, a operação *XOR* entre o Qubit de controle e o Qubit alvo é armazenado no Qubit alvo. Existem muitas outras portas para sistemas de 2 Qubits, ou mesmo sistemas maiores, no entanto a porta *C-NOT* junto com portas de 1 Qubit são protótipos para todas as outras portas, por causa do resultado notável sobre universalidade das portas: *Qualquer porta lógica de múltiplos Qubits pode ser construída a partir da porta NÃO - Controlada e das portas de um Qubit*[12].

Como exemplo podemos ver na figura 6 uma porta de *Troca* que faz justamente a troca dos estados entre os dois Qubits, as operações podem ser acompanhadas na equação abaixo:

$$\begin{aligned} |\mathbf{a},\mathbf{b}> &\mapsto |\mathbf{a},\mathbf{a}\oplus\mathbf{b}> \\ &\mapsto |\mathbf{a}\oplus(\mathbf{a}\oplus\mathbf{b})>=|\mathbf{b},\mathbf{a}\oplus\mathbf{b}> \\ &\mapsto |\mathbf{b},(\mathbf{a}\oplus\mathbf{b})\oplus\mathbf{b}>=|\mathbf{b},\mathbf{a}> \end{aligned} \quad (4.6)$$

A figura 6 nos dá a idéia de um *Circuito Quântico* ele é representado por fios que indicam a passagem de cada Qubit atravessando as portas quânticas. Existem algumas ações que não são permitidas nos circuitos quânticos, por exemplo a realimentação, permitida em circuitos lógicos clássicos, diz-se que os circuitos quânticos são acíclicos. Portas para n Qubits podem ser construídas conforme apresentado na figura 7.

Um último circuito importante, não que os demais sejam menos importantes, é o circuito para medir o Qubit. Segundo os postulados da mecânica quântica[13], a medida M de um observável $|\mathbf{\Psi}>$ somente é determinística se for um

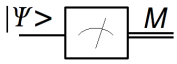

Figura 8: Circuito para medir o valor de um Qubit

dos auto-estados (estado fundametal), assim os comandos de teste não são mais resultados booleanos do sistema e sim operações de medidas probabilísticas. A medida do Qubit, deve resultar, no entanto, o valor *0*, ou *1*, a medida de um estado quântico deve resultar um valor clássico. A figura 8 indica um circuito onde os Qubits são representados por linha simples enquanto que os valores medidos para o sistema e indicados por bits clássicos são representados por linhas duplas. Devemos lembrar que a medida obtida do Qubit que está no estado $|\psi>=\alpha|\mathbf{0}>+\beta|\mathbf{1}>$ tem probabilidade α^2 de ser o valor *0* e β^2 de ser o valor *1*, mas somente um valor será medido.

5. JUNTANDO OS PEDAÇOS

Na seção anterior nós vimos uma introdução à construção de circuitos quânticos que permite dar os primeiros passos para a construção da arquitetura. Por exemplo, podemos ver na figura 9 a construção de um circuito que realiza a "soma" de Qubits. Podemos imaginar, então, que a construção de um computador quântico é realizada integrando as diversas portas quânticas em uma rede quântica. No entanto várias complicações surgem[7], primeiro, não existe o similar a um *fio metálico* que permita ligar as portas e carregar os Qubits, muito pelo contrário, os Qubits no deslocamento podem interagir com o ambiente alterando seu estado em um processo chamado *Descoerência*, é necessário um processo específico para transporte dos voláteis Qubits. De acordo com o teorema de não-clonagem[7] é impossível criar uma cópia exata de um Qubit arbitrário $\alpha|\mathbf{0}>+\beta|\mathbf{1}>$, o teorema de não clonagem possui conseqüências severas no transporte quântico. Cada Qubit precisa ser movido ponta a ponta e não copiado, desta forma é necessário construir *fios* confiáveis para este transporte. A idéia simplista de arremessar um Qubit da origem ao destino é impraticável, pois o efeito de Descoerência pode ocorrer em vários momentos, na saída, ao longo do caminho e também na entrada, logo o Qubit recebido não estará no estado inicial em que se pretendia transmitir. Uma proposta[7] mais viável é o uso da operação de troca, vários Qubits alinhados operam a troca de forma que a informação de um Qubit saia da origem e atinja o último Qubit. O problema Ãl' que precisaríamos de uma rede de portas quânticas, isto poderia aumentar o problema de Descoerência. Um outro mecanismo importante é o teleporte quântico. Tanto a rede de troca quanto o teleporte são viáveis no transporte da informação, mas ambos apresentam problemas, uma rede de troca não pode ser muito longa, pois o efeito da descoerência acaba afetando o Qubit, isto impõe um limitante máximo para o caminho, e o teleporte implica em um mecanismo maior inserido no caminho, o que limita o comprimento mínimo do caminho.

5.1 Teleporte Quântico

A figura 10 apresenta um circuito que realiza o teleporte, onde é necessário um par EPR para funcionar. O estado do Qubit incial que desejamos teleportar é $|\mathbf{\Psi}>$. Vamos trabalhar com um sistema que utiliza o par EPR conhecido

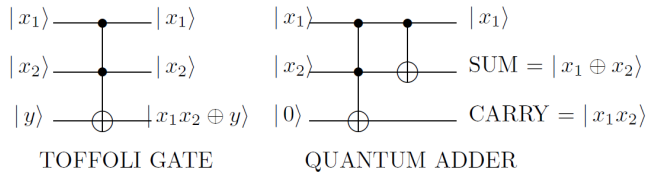

Figura 9: Circuito de um somador quântico[3]

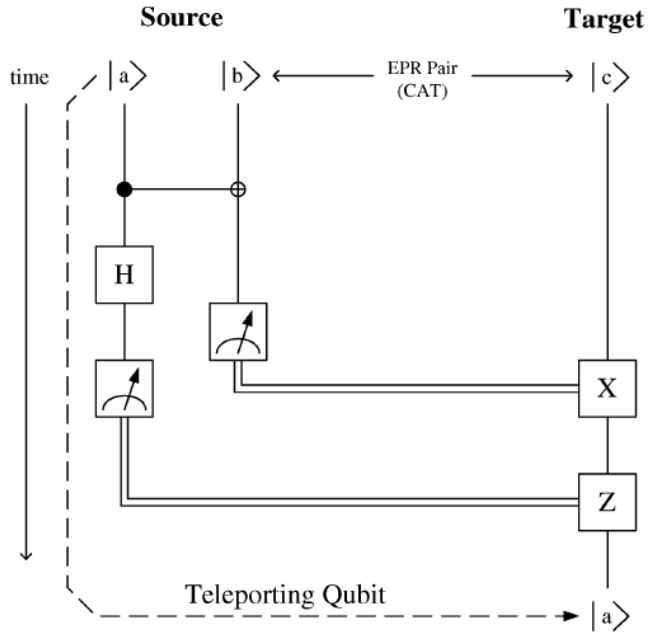

Figura 10: Circuito Quântico de Teleporte[7]

como: $|\beta_{00}>$. O estado geral do sistema que envolve o Qubit original e o par EPR $|\Psi_0>$ é:

$$|\Psi_0> = |\mathbf{\Psi}> |\beta_{00}> = \frac{1}{\sqrt{2}}[\alpha|0>(|00>+|11>)+\beta|1>(|00>+|11>)] \quad (5.1)$$

O par EPR em um Estado de Bell é responsável pelo teleporte, o primeiro Qubit está associado à origem e o segundo Qubit do par está associado ao destino, vemos na figura 10 esta correlação. A equação (5.1) na sua última linha apresenta o sistema inicial, associando o estado original do Qubit a ser teleportado com o par EPR. Os dois primeiros Qubits representam a origem, e o terceiro Qubit o destino. Ao aplicar *C-NOT* com o Qubit $|\mathbf{\Psi}>$ como controle da porta *NÃO* atingimos o estado $|\Psi_1>$ para o conjunto:

$$|\Psi_1> = \frac{1}{\sqrt{2}}[\alpha|0>(|00>+|11>)+\beta|1>(|10>+|01>)] \quad (5.2)$$

Observe que na probabilidade (β^2) do estado original ser 1, o primeiro bit do par EPR foi trocado através da porta *NÃO*. Agora aplicamos a porta *Hadamard* sobre o bit original, ficamos com o estado $|\Psi_2>$:

$$|\Psi_2> = \frac{1}{2}[\alpha(|0>+|1>)(|00>+|11>) + \beta(|0>-|1>)(|10>+|01>)] \quad (5.3)$$

Este resultado pode ser reescrito como:

$$|\Psi_2> = \frac{1}{2}[|00>(\alpha|0>+\beta|1>)+|01>(\alpha|1>+\beta|0>) + |10>(\alpha|0>-\beta|1>)+|11>(\alpha|1>-\beta|0>)] \quad (5.4)$$

Após a medida dos dois Qubits que descrevem o estado na origem representado na equação (5.4) teremos somente o último Qubit em um estado quântico: $|\mathbf{\Psi}_3>$, neste caso, seu estado é decorrente da correlação existente no par EPR, o estado $|\mathbf{\Psi}_3>$, será representado por apenas uma das quatro parcelas da soma acima. A tabela 2 indica qual o estado final de $|\mathbf{\Psi}_3>$ de acordo com o estado lido para os dois primeiros Qubits. Para que o estado final do Qubit no destino seja o estado do Qubit original deve-se operar troca de fase de acordo com os valores medidos, se o estado medido for $|00>$ então o estado de $|\mathbf{\Psi}_3>$ já é uma cópia do estado original teleportado, se o estado medido for $|01>$ para atingir o estado original é necessário fazer $|\mathbf{\Psi}_3>$ passar por uma porta X, se for $|10>$ deve-se passar por uma porta Z e se a medida indicar o estado $|11>$ deve-se passar pelas portas X e Z em seqüência. Alguns pontos interessantes

$$|\mathbf{00}> \equiv \alpha|0>+\beta|1>$$
$$|\mathbf{01}> \equiv \alpha|1>+\beta|0>$$
$$|\mathbf{10}> \equiv \alpha|0>-\beta|1>$$
$$|\mathbf{11}> \equiv \alpha|1>-\beta|0>$$

Tabela 2: Estado do Qubit teleportado após a realização da medida nos Qubits originais

no teleporte: é necessária uma medida clássica para que ele funcione, por outro lado a medida clássica impõe restrição na velocidade, não é possível teleportar um Qubit em velocidades superiores à velocidade da luz, decorrente disto, não é possível teleportar uma informação para o passado (seguindo os preceitos da teoria da relatividade)[12]. Outro fato é que o teleporte não é uma cópia do estado de um Qubit, pois o Qubit original se perdeu a partir do momento em que foi realizada a medida, restando somente o segundo Qubit do par EPR original em um estado quântico idêntico ao estado do Qubit original.

5.2 Construindo a Arquitetura

Para construir uma arquitetura com base nas portas lógicas quânticas, enfrentamos para o transporte e armazenamento do Qubit o problema da descoerência, o estado de um Qubit é volátil, e ele se perde principalmente por interação com o ambiente ou outra fonte de ruídos. Para uma arquitetura viável é necessário mecanismos de correção dos Qubits a fim de evitar resultados incorretos decorrente da descoerência. Esta tarefa apresenta duas dificuldades[14]: a correção de um Qubit difere de um bit clássico, pois o estado de um Qubit é uma distribuição probabilística de um estado quântico, os erros ocorrem em um contínuo e não em um valor discreto como em bits clássicos, pequenas mudanças de fase já são fontes de erro. Outro motivo de dificuldade é o fato de que o estado deve ser corrigido sem que tenhamos conhecimento de qual é o estado, pois qualquer medida irá colapsar em um valor de estado fundamental.

Existe um mecanismo de correção eficiente[14], utiliza-se um código $[n, k]$, onde n Qubits são utilizados para codificar k

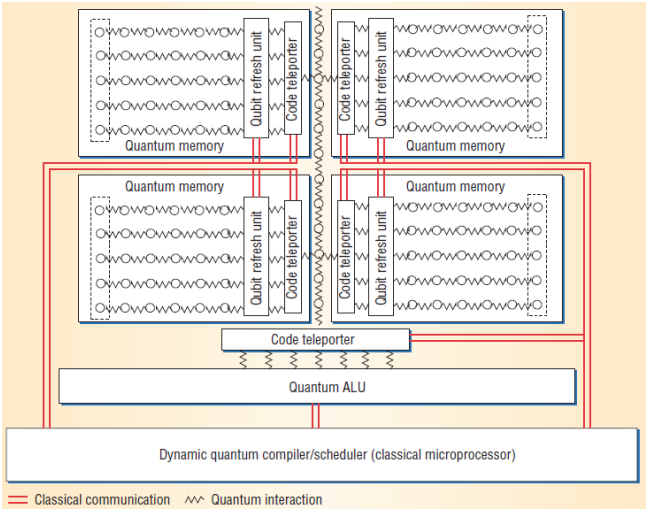

Figura 11: Proposta de Arquitetura de Computador Quântico[14]

Qubits de dados. O circuito de correção de erro utiliza k Qubits de dados e $n-k$ Qubits auxiliares, estes são construídos a partir do estado $|\mathbf{0}>$. A decodificação verifica os n Qubits, k são Quits de dados possivelmente errôneos, e $n-k$ Qubits que, com grande probabilidade, descreve o erro ocorrido. O circuito de correção então aplica uma das 2^{n-k} operações para corrigir o erro. O custo do mecanismo de correção de erro é sobrecarga necessária para criar os estados codificados e executar os passos periódicos de correção de erro, cada passo é uma operação tolerante a falhas[14], no entanto a eficiência é alta. Esta técnica aplicada recursivamente consegue que a taxa de erro caia exponencialmente com um custo polimonial do circuito de correção de erro.

Uma proposta de arquitetura de computador quântico[14] pode ser vista na figura 11, construída com base em caminhos de dados confiáveis e memória quântica eficiente. Podemos notar que a estrutura da arquitetura para computação quântica é semelhante à classica, no entanto alguns aspectos são únicos do domínio quântico. Como a fiura 11 mostra, são definidos três componentes principais: A unidade lógica-aritmética quântica (ULA), memória quântica e um escalonador dinâmico. É necessário usar a técnica de teleporte no transpore da informação quântica.

A construção de um mecanismo de memória confiável recai no uso de sistemas que oferecem uma taxa baixa de descoerência para Qubits estáticos, mesmo assim, tal qual uma memória RAM, que "vaza" ao longo do tempo, o Qubit armazenado ainda sofre a descoerência, estes dispositivos necessitam de unidades de *refresh*, que são menos complexas que uma ULA, mas também necessitam portas quânticas para gerar a correção de erro. O mecanismo de refresh oferece a confiabilidade necessária para o conjunto de memória, no entanto, como são necessários muitos Qubits para garantir a confiabilidade de um segundo o mecanismo de correção de erro, são necessários vários módulos de memória.

A ULA no núcleo da arquitetura executa as operações, tanto para computação, quanto para correção de erro. Ela é composta de um conjunto básico de portas quânticas:

- Hadamard
- Identidade (I, ou NOP quântico)
- Flip de Bit (X, ou NÃO quântico)
- Flip de Fase (Z)
- Flip de Bit e Fase (Y)
- Rotação por $\pi/4$ (S)
- Rotação por $\pi/8$ (T) e
- NÃO - controlado (C-NOT)

Estas portas formam o menor conjunto universal possível[14]. As portas operam sobre dados codificados por correção de erro para garantir computação tolerante a falhas. Como são necessários os Qubits auxiliares para a codificação e aplicação da correção de erro, um hardware específico deve gerar os Qubits em estados elementares que serão utilizados pela ULA.

O transporte da informação é um desafio, como vimos, não é possível clonar um Qubit, então optou-se por usar o mecanismo de teleporte, pois a rede de portas de troca acaba inserindo um ruído muito grande, comparado com o mecanismo de teleporte. O mecanismo de teleporte utiliza rede de portas de troca para transportar um dos bits do par EPR para o destino, para tanto não é necessário o uso de correção de erro, os bits do par EPR podem ser verificados facilmente por erro e independente do Qubit físico a ser transmitido, ele pode ser descartado se houver erro e um novo par gerado. Uma vez o par correto, um Qubit do par na origem e outro no destino, o bit físico pode ser teleportado através da distância desejada.

Esta arquitetura prevê um processador clássico de alta performance no controle de escalonamento dinâmico. Este usa construções clássicas de controle de fluxo e dinamicamente traduz as operações lógicas em operações sobre Qubits físicos individuais. O algoritmo em execução utiliza o tamanho dos dados de entrada e as taxas de erros para os Qubits físicos para construir um controle de escalonamento dinâmico a fim de controlar a ULA quântica, o teleporte de códigos e o *refresh* das unidades da RAM baseadas em Qubits.

6. FUNCIONA ?

Algumas são as possibilidades abertas para construção de computadores quânticos, porém apenas três representações fundamentais de Qubits são utilizadas[12]: o *spin*, a carga e o fóton. Existem quatro requisitos básicos para a implementação da computação quântica: representação dos Qubits, Evolução unitária controlável (operação das portas quânticas), preparação dos estados iniciais (como para criar o par EPR) e a medida do estado final dos Qubits. Abaixo uma breve descrição das propostas de implementações:

Computador Quântico Ótico: o Qubit é representado pela localização de um único fóton em duas cavidades representadas pelos modos: $|01>$ e $|10>$, ou mesmo pela sua polarização. As portas e trasnformações são construídas de deslocadores de fase, divisores de feixe e meios não-lineares

que permite a modulação relativa de dois fótons. A dificuldade está na construção dos meios não-lineares.

Eletrodinâmica Quântica de Cavidades Óticas - EDQ: baseado no acoplamento de um único átomo com alguns poucos modos óticos através do confinamento de átomos em cavidades com altos valores de Q (fator de qualidade), nestas cavidades os átomos apresentam estados eletromagnéticos (fótons), a representação dos Qubits é dada pela localização de um único fóton entre dois modos. As portas são construídas da mesma forma que no Computador Ótico. A dificuldade também está no acoplamento de dois fótons, neste caso mediado por um átomo.

Armadilhas Iônicas: uma das formas mais promissoras, os átomos aprisionados são resfriados até que sua energia cinética permite a distinção dos estados de spin do núcleo e do elétron, os estados quânticos são representados pelos Spins: $-\frac{3}{2}$, $-\frac{1}{2}$, $\frac{1}{2}$ e $\frac{3}{2}$, que podem representar 2 Qubits em seus quatro estados. As portas são construídas a partir de aplicações de pulsos de laser que manipulam os estados atômicos externamente. As dificuldades são: o tempo de descoerência pois o tempo de vida dos fônons (estado de vibração dos *spins*) é muito curto, e preparar os íons no estado fundamental é uma tarefa difícil.

Ressonância Magnética Nuclear: A representação dos Qubits se dá pelo *spin* de um núcleo atômico e sua precessão pela aplicação de campos magnéticos fortes. As portas são construídas pela aplicação de pulsos de campo magnético em um forte campo magnético estático. A dificuldade ocorre na preparação dos estados fundamentais e na leitura, o sinal de precessão é extremamente fraco.

Outros esquemas são previstos, apesar do alarde da Canadense D-Wave Systems[2] de já ter construído computador com base em 128 Qubits, a comunidade acadêmica se restringe a reconhecer propostas que evidenciam algumas naturezas quânticas principais, como teleporte ou estados EPR, os protótipos existentes definem computadores que chegam a uma dezena de Qubits. O quadro da figura12 mostra as perspectivas de futuro para a computação quântica.

QC Approach	The DiVincenzo Criteria						
	Quantum Computation					QC Networkability	
	#1	#2	#3	#4	#5	#6	#7
NMR							
Trapped Ion							
Neutral Atom							
Cavity QED							
Optical							
Solid State							
Superconducting							
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.						

Legend:
= Uma abordagem viável potencial atingiu prova suficiente do princípio
= Uma abordagem viável potencial foi proposta, mas não há prova suficiente do princípio
= Não é conhecida nenhuma abordagem
#1 = Um sistema físico escalável com Qubits bem caracterizados
#2 = Habilidade de iniciar Qubits em um estado simples garantido
#3 = Tempo de descoerência longo, muito maior que o tempo de operação da porta
#4 = Um conjunto universal de portas quânticas
#5 = Capacidade de medir específicos Qubits
#6 = Capacidade de trocar Qubits estacionários e em movimento
#7 = Capacidade de transmitir de forma segura Qubits em movimento entre posições específicas

Figura 12: Perspectivas da Computação Quântica[6]

7. CONCLUSÃO

A computação quântica é uma proposta de ferramenta poderosa na solução de problemas computacionais impraticáveis no âmbito do poder computacional atual. A fundamentação física comprova a possibilidade da implementação do equipamento, e protótipos já demonstram uma viabilidade prevista no desenvolvimento dos dispotivos, no entanto o desenvolvimento destes equipamentos ainda é muito incipiente. A promessa é para o futuro, mas com base na evolução tecnológica recente, o futuro pode estar bem próximo.

8. REFERÊNCIAS

[1] Baggot, J. *Beyond Measure – Modern Physics, Pylosophy and the Meaning of Quantum Theory.* Oxford University Press, 2004.

[2] Cormen, T. H., Leiserson, C. E., Rivest, R. L., and Stein, C. *Algoritmos - Teoria e Prática.* Elsevier Editora Ltda., 2002.

[3] Ekert, A., Hayden, P. M., and Inamori, H. *Basic Concepts in Quantum Computation*, vol. 72/2001 of *Les Houches*. Springer Berlin / Heidelberg, 2001.

[4] Heisenberg, W. *The Physical Principles of the Quantum Theory – Translated by Eckart C. and Hoyt F. C.* Dover Publications, 1949.

[5] Hennessy, J. L., and Patterson, D. A. *Arquitetura de Computadores - Uma Abordagem Quantitativa*, 4 ed. Elsevier Editora Ltda., 2008.

[6] Hughes, R., et al. A quantum information science and technology roadmap - part 1: Quantum computation. http://qist.lanl.gov/ acessado em Maio, 2010.

[7] Isailovic, N., et al. Data path and control for quantum wires. *ACM Transactions on Architecture and Code Optmization (TACO) 1*, 1 (Mar. 2004), 34–61.

[8] Massimi, M. *Pauli's Exclusion Principle - The Origin and Validation of a Scientific Principle.* Cambridge University Press, 2005.

[9] Maxwell, J. C. *A Treatise on Electricity and Magnetism: Unabridged 3rd Edition, 2 Volumes Bound as One.* Dover Publications, 1954.

[10] Moore, G. E. Cramming more components onto integrated circuits, reprinted from electronics, volume 38, number 8, april 19, 1965, pp.114 ff. *Solid-State Circuits Newsletter, IEEE 20*, 3 (Sept. 2006), 33–35.

[11] Newton, I. *The Principia - Mathematical Principles of Natural Philosophy - A new translation by Cohen, I. B. and Whitman, A.* University of California Press, 1999.

[12] Nielsen, M. A., and CHang, I. L. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[13] Ömer, B. *Structured Quantum Programming.* PhD thesis, Institute for Theoretical Physics - Vienna University of Technology, 2009.

[14] Oskin, M., Chong, F. T., and Chuang, I. L. A practical architecture for reliable quantum computers. *Computer 35*, 1 (jan 2002), 79–87.

[15] Rae, A. *Quantum Physics - Illusion or Reality?* Cambridge University Press, 1986.

[2] http://www.dwavesys.com/