# Introdução à Computação Quântica

Hamilton José Brumatto - RA: 096389
brumatto@ic.unicamp.br

Universidade Estadual de Campinas - SP

14 de junho de 2010

# Sumário


- Física Clássica x Física Quântica
- O Princípio da Incerteza
- O Bit Quântico - Qubit
- *n* Qubits
- Porta Lógica de um Qubit
- Porta Lógica de *n* Qubits
- Circuito Lógico Quântico
- ULA Quântica
- Arquitetura de Computador Quântica
- Computadores Quânticos
- Conclusão

Como entender a Física Quântica?

- Física Clássica = Newton + Maxwell
- Fatos não são explicados:
  - Elétrons não caem no núcleo.
  - Catástrofe do Ultravioleta.
- Quanta: valores discretos de energia: $E = nh\nu$ (Planck)
- Física Quântica: Nível atômico possui níveis quânticos

Dualidade Partícula-Onda

- Heisenberg compila resultados:
  - Raios $\beta$: partícula em câmera de bolha
  - Raios $\beta$: onda ao atravessar estrutura cristalina
  - Raios X: onda ao atravessar estrutura cristalina
  - Raios X: partícula ao atravessar vapor supersaturado
- Princípio da incerteza:
  - Não é possível conhecer posição e velocidade ao mesmo tempo:
  - $\Delta x \cdot \Delta p \geqslant \frac{h}{4\pi}$
- Einstein: Efeito partícula onda na Luz - *fótons*
- Figura de difração: fótons um a um.
- **A medida influi no estado da partícula**

Estados Quânticos Fundamentais: Qubits

- Sistema possui dois estados ortogonais:
  - $|\mathbf{0}>$ e $|\mathbf{1}>$
  - $<\mathbf{0}|\mathbf{0}>=1$, $<\mathbf{1}|\mathbf{0}>=0$, $<\mathbf{0}|\mathbf{1}>=0$ e $<\mathbf{1}|\mathbf{1}>=1$
- Princípio da incerteza: Em qual estado está o sistema?
  - Estado é representado por uma função de probabilidade:
  - $|\psi>=\alpha|\mathbf{0}>+\beta|\mathbf{1}>$
  - $\alpha^2+\beta^2=1$
  - $\alpha^2$ e $\beta^2$ representam a probabilidade
- Exemplo: Elétron na camada *s* do átomo de hidrogênio
- **Um Qubit medido estará em um estado fundamental**

Estados de sistemas com 2 Qubits

- Cada Qubit está em um estado:
  - $\psi >= \alpha|\mathbf{0}> + \beta|\mathbf{1}>$ e $\phi >= \eta|\mathbf{0}> + \delta|\mathbf{1}>$

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

- Sistema com quatro estados quânticos representa sistema de 2 Qubits

- Estados fundamentais são auto-estados, representados por auto-vetores.

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

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

- Se um Qubit for medido no estado $m$:

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

- Estado de Bell, ou par EPR:

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

- Sitemas com $n$ Qubits: $2^n$ estados:

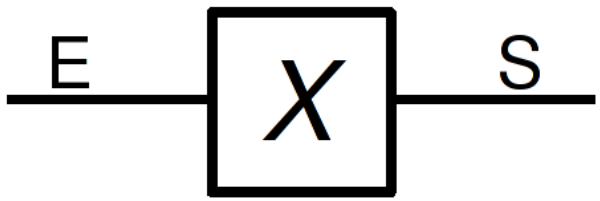
$$|\mathbf{\Psi}> = |\psi_1> \otimes |\psi_2> \otimes |\psi_3> \otimes \ldots \otimes |\psi_n>$$

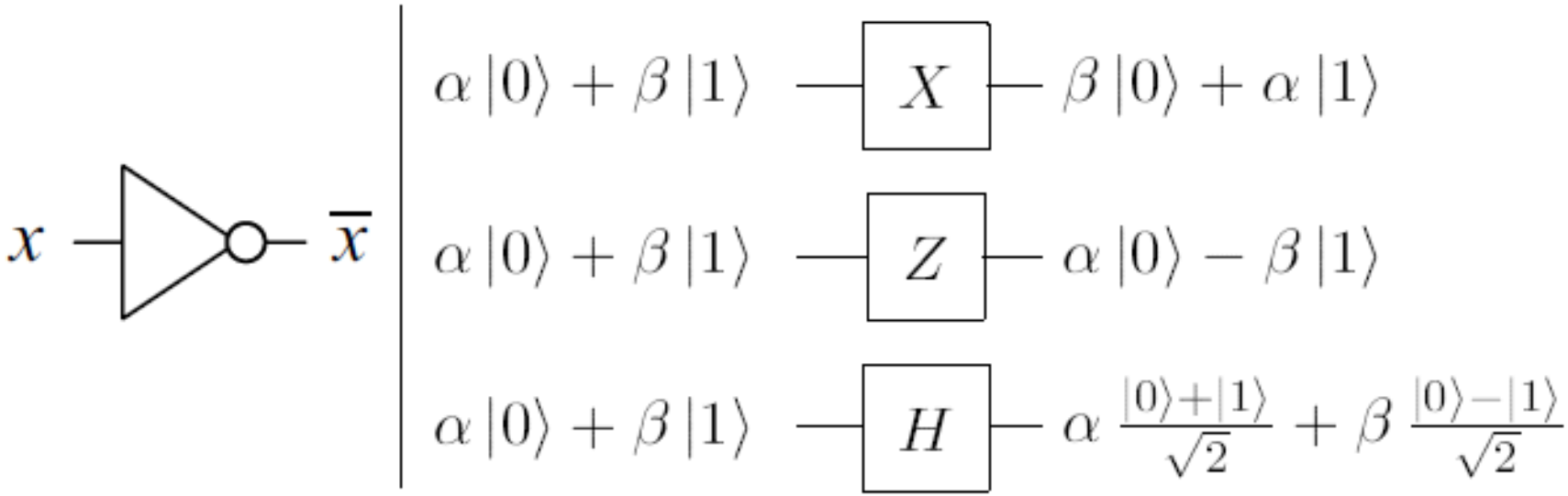
Poder computacional previsto para a Computação Quântica.

- Sistema com $n$ Qubits possui $2^n$ estados.
- Medida representa apenas um estado, dada a probabilidade na distribuição.
- Modelo próprio para a Máquina Probabilística de Turing.
- Algoritmos conseguem resover problemas NP-Completos em tempo polinomial.

- Transforma estado $|\mathbf{0}>$ em $|\mathbf{1}>$ e vice-versa.

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






- A porta *H*, porta de *Hadamard*, é conhecida como "raiz quadrada de NÃO"
- A porta quântica deve ser unitária

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

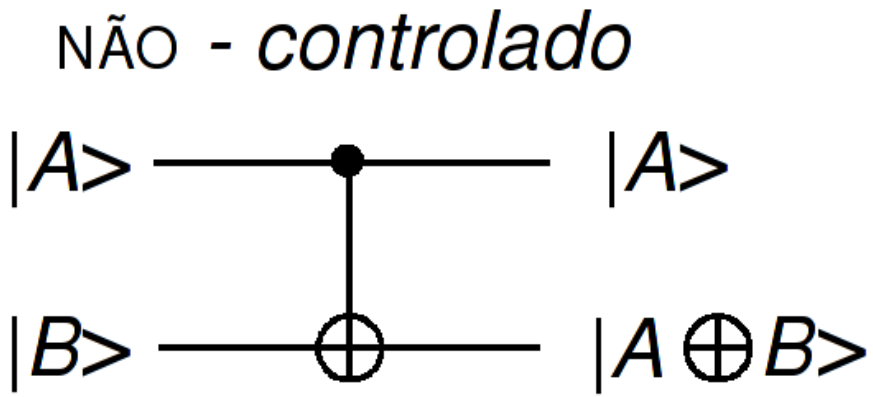
$$Pauli - Y \quad : \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Fase \quad : \quad S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$\frac{\pi}{8} \quad : \quad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

- Portas *Pauli-X*, *Pauli-Y* e *Pauli-Z*: Portas de Inversão
- Porta $H$ - (*Hadamard*), $S$ - (de *Fase*) e $T$ - $(\pi/8)$: Deslocamento de Fase
- A porta $S$ (Fase) é a raiz quadrada da porta $Z$ de Pauli
- A porta $T$ $(\pi/8)$ é a raiz quadrada da porta de Fase.

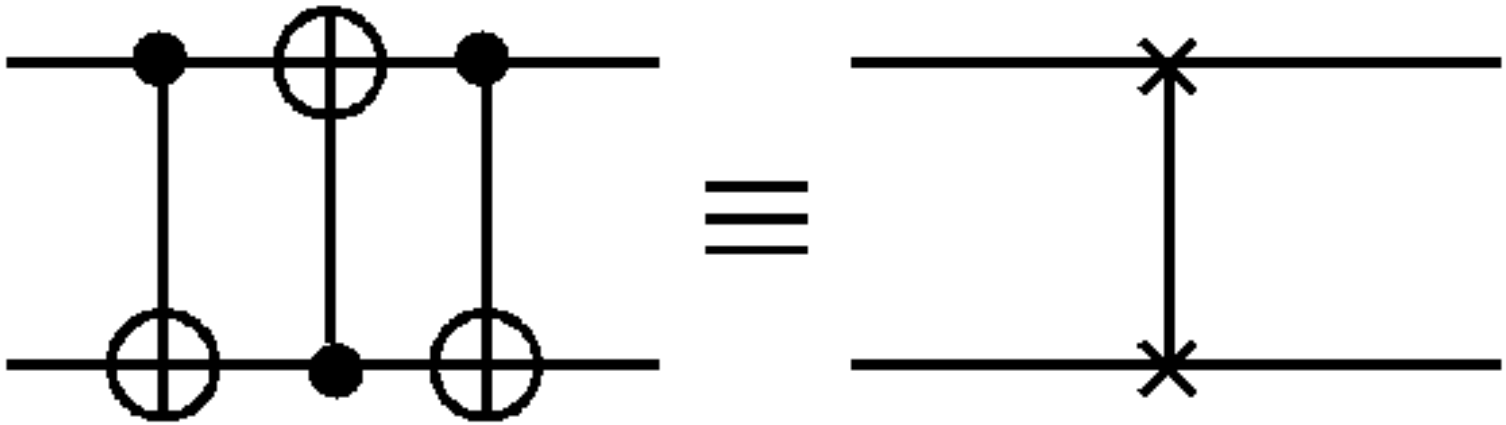
- Porta NÃO-Controlado: C-NOT




$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

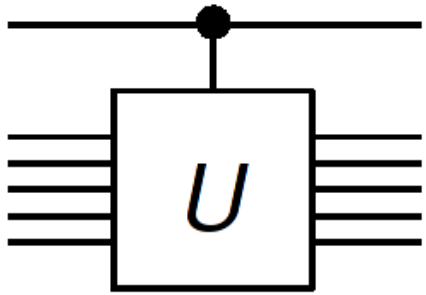
- Existem outras portas de 2 Qubits
- Porta C-NOT junto com portas de um Qubit forma conjunto universal
- Porta de $n$ Qubits é representada por matriz de $2^n x 2^n$

- Porta de Troca: Circuito com portas C-NOT.

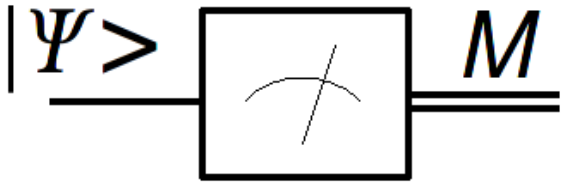


$$
\begin{aligned}
|\mathbf{a}, \mathbf{b}> &\mapsto |\mathbf{a}, \mathbf{a} \oplus \mathbf{b}> \\
&\mapsto |\mathbf{a} \oplus (\mathbf{a} \oplus \mathbf{b}) >= |\mathbf{b}, \mathbf{a} \oplus \mathbf{b}> \\
&\mapsto |\mathbf{b}, (\mathbf{a} \oplus \mathbf{b}) \oplus \mathbf{b} >= |\mathbf{b}, \mathbf{a}>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

- Porta Controlada de *n* Qubits

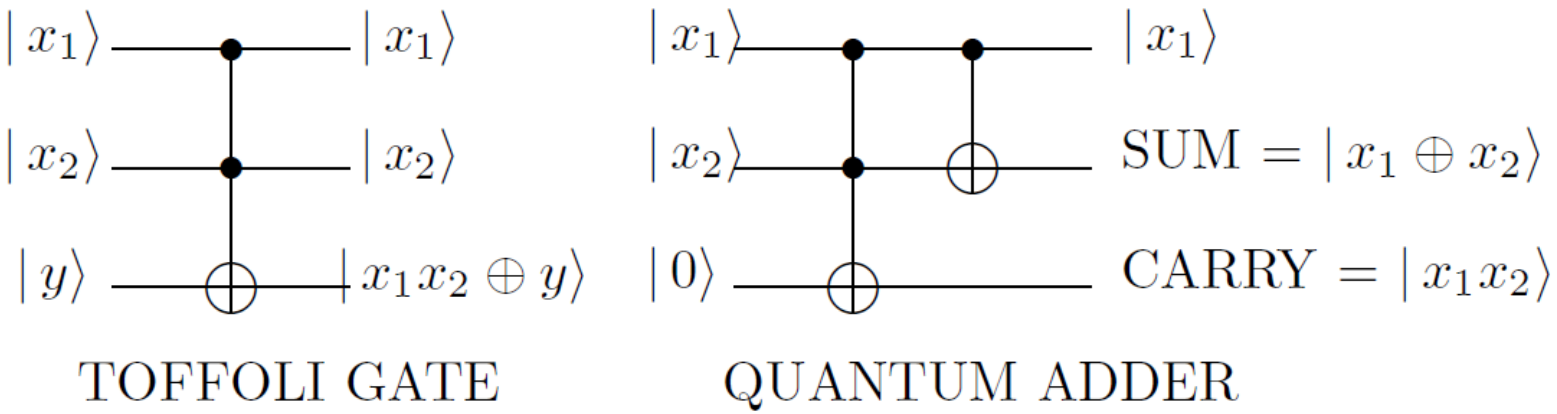



- Circuito de medida (obtém valor clássico)

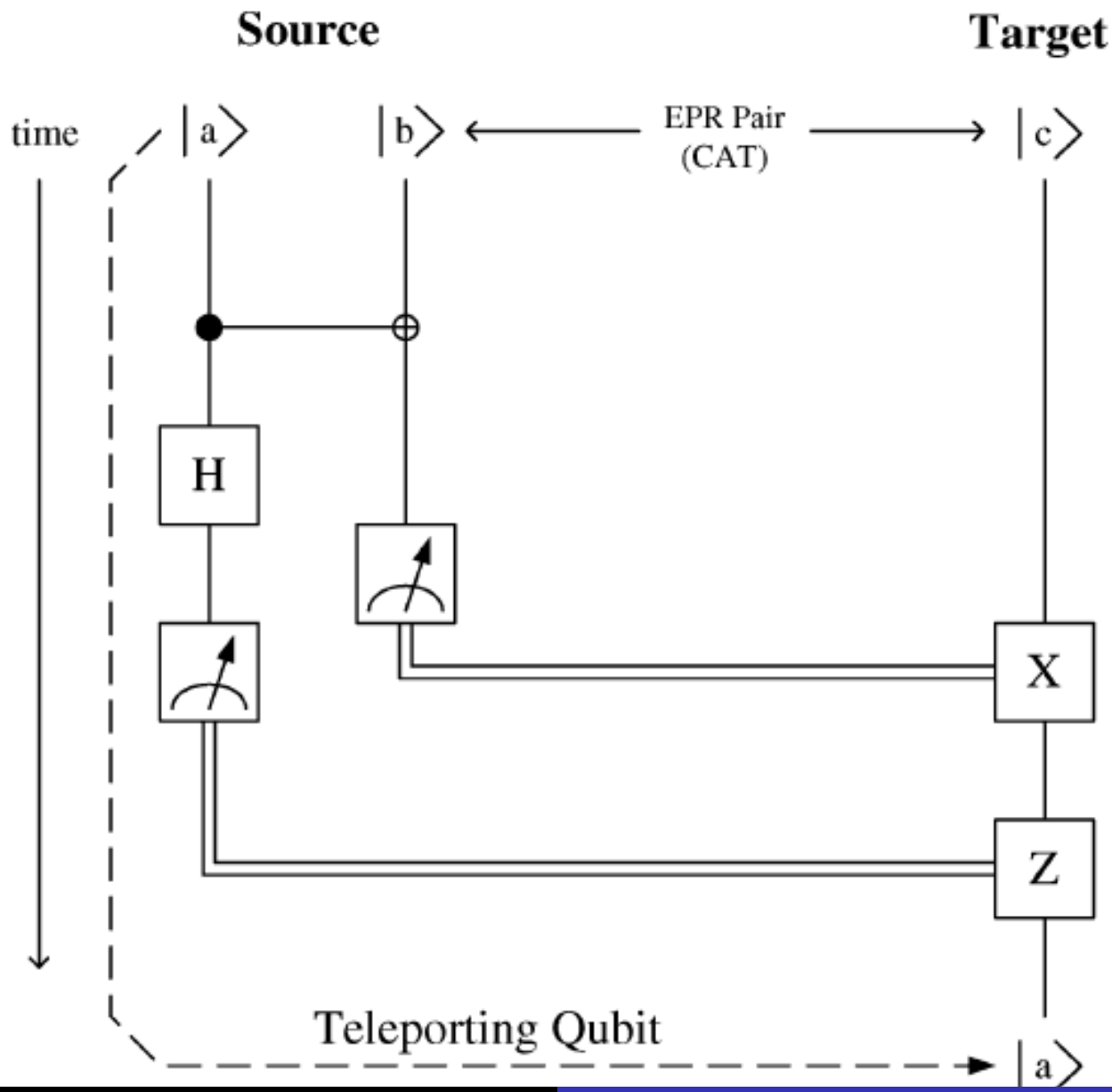



- Um único valor de estado fundamental medido
- $|\psi>=\alpha|\mathbf{0}>+\beta|\mathbf{1}>$: probab. $\alpha^2$ de ser *0* e $\beta^2$ de ser *1*

- Rede de Portas Quânticas: Adder




- Problema de **Descoerência** no transporte de Qubits
- Mecanismos de transporte confiáveis:
  - Rede de portas de troca
  - Teleporte Quântico


Source
Target
time
|a⟩
|b⟩
EPR Pair
(CAT)
|c⟩
H
X
Z
Teleporting Qubit
|a⟩

- Par EPR responsável pelo teleporte

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

- Teleporte Quântico : Porta C-NOT e Hadamard

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

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

- Teleporte Quântico : Reescrevendo o resultado

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

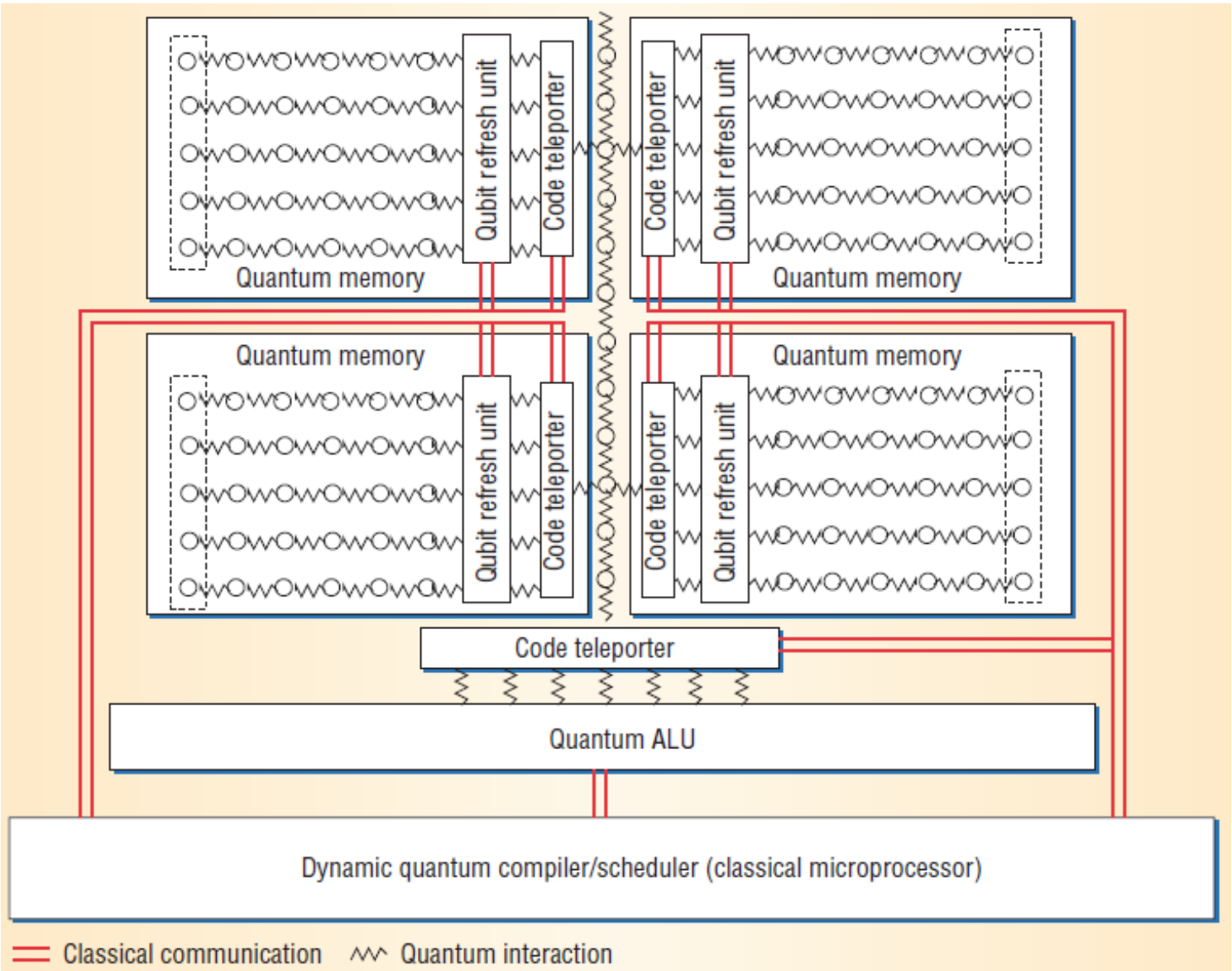
$$
\begin{aligned}
|\Psi_2> = & \\
& \frac{1}{2}[|00>(\alpha|0>+\beta|1>)+|01>(\alpha|1>+\beta|0>) \\
& +|10>(\alpha|0>-\beta|1>)+|11>(\alpha|1>-\beta|0>)]
\end{aligned}
$$

- Após a medida do Qubit original e primeiro Qubit do par EPR resta possivelmente uma inversão.

Evitando a Descoerência

- O estado deve ser corrigido para o original sem termos conhecimento do original
- Código $[n, k]$, $k$ Qubits de dados.
- $n - k$ Qubits auxiliares incialmente no estado fundamental $|\mathbf{0}>$.
- Após a operação quântica, o estado dos Qubits auxiliares representam o erro de descoerência.
- Aplica-se uma das $2^{n-k}$ operações de correção do erro.
- Custo do mecanismo: sobrecarga de Qubits e operações.

# Arquitetura Quântica
## Arquitetura Proposta[4]



- Memória Quântica: Necessita correção de erro e *refresh*.
- ULA Quântica: Conjunto universal de portas quânticas.
- ULA realiza operações quânticas e operações de correção de erro.
- Circuito de teleporte quântico para transporte de Qubits.
- Circuito de controle baseado em processador clássico de alto desempenho.

ULA Quântica

- 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)

Computador Quântico Ótico

- Qubit: localização de um único fóton em duas cavidades: $|01>$ e $|10>$
- Qubit: polarização do fóton.
- Portas: tranformações baseada em deslocadores de fase, divisores de feixe e meios não lineares para modulação relativa de dois fótons.
- Meios não lineares apresentam a dificuldade para o modelo.

Eletrodinâmica Quântica de Cavidades Óticas - EDQ

- Acoplamento de um único átomo com alguns modos óticos confinado em cavidade com alto valor de Q (fator de qualidade)
- Qubit: Fótons do estado ótico do átomo
- Portas: semelhante ao computador ótico.
- Meios não lineares representam, também, a dificuldade para este modelo.

Armadilhas Iônicas

- Átomos resfriados até que a energia cinética permita distinção entre estados de *spin*
- Qubit: Acoplamento de Spin: elétron-núcleo: $-\frac{3}{2}$, $-\frac{1}{2}$, $\frac{1}{2}$ e $\frac{3}{2}$
- Portas: pulsos de laser para manipulação dos estados atômicos.
- Dificulades: tempo de descoerência dos fônons (estado de vibração dos *spins*) e preparar íons no estado fundamental.
- Modelo mais promissor.

Ressonância Magnética Nuclear

- Átomos precessionando na aplicação de um campo magnético estático intenso.
- Qubit: *Spin* do núcleo em precessão.
- Portas: pulsos magnéticos em um forte campo magnético estático.
- Dificuldades: medida de estado, o sinal de precessão é muito fraco e preparação do estado fundamental.

- Existem outros modelos.
- Máquinas atingem próximo de uma dezena de Qubits.
- Alarde da D-Wave Systema de computador quântico de 128 Qubits não reconhecido.
- Roadmap criado em 2004 para evolução até 2012.

# Computadores Quânticos
## Roadmap[1]

| 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

- Proposta de ferramenta poderosa no solução de problemas computacionais intratáveis.
- Fisicamente possível.
- Protótipos demonstram uma viabilidade prevista.
- Resultados muito pequenos atualmente.
- Depende da evolução tecnológica, a história garante que é promissor.

# Referências


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

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.

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

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