

# Computação e informação quânticas

**A. Sernadas<sup>+</sup>**

com a colaboração de

**P. Mateus<sup>+</sup> e Y. Omar<sup>++</sup>**

**+ CLC, Dep. Matemática, IST, UTL**

Av. Rovisco Pais, 1049-001 Lisboa, Portugal

{acs,pmat}@math.ist.utl.pt

**++ CEMAPRE, Dep. Matemática, ISEG, UTL**

Rua do Quelhas 6, 1200-781 Lisboa, Portugal

yomar@iseg.utl.pt

Simpósio

*A Investigação na Universidade Técnica de Lisboa*

IST, 2 e 3 de Fevereiro de 2006

# 1 Inevitabilidade da computação/comunicação quântica

2

- **Miniaturização crescente dos circuitos clássicos:**  
relevância dos efeitos quânticos cada vez mais próxima...
- **Existência de processos quânticos não simuláveis de modo eficiente com computadores clássicos:**  
por que não tentar usar processos quânticos desse tipo para obter computadores mais rápidos?
- **Entrelaçamento permite correlação à distância:**  
por que não tentar usar esse efeito em problemas de sincronização?

## 2 Alguns marcos

3

- Proposta de Benioff (1980): máquina de Turing quântica;
- Proposta de Feynman (1982): computação quântica;
- Protocolo de Bennett e Brassard (1984): partilha de chaves privadas;  
Protocolo de Ekert (1991): idem usando entrelaçamento;
- Proposta de Deutsch (1985): computador quântico universal;
- Protocolo de Bennett e Wiesner (1992): codificação densa;
- Protocolo de Bennett et al (1993): teleportação quântica;
- Algoritmo de Shor (1994): decomposição em factores primos;
- Algoritmo de Grover (1995): pesquisa em bases de dados;

- Teorema de DiVincenzo (1995): portas quânticas universais;
- Teorema de Schumacher (1993/1995): 1o. teorema de Shannon para canais quânticos;
- Shor (1995) and Steane (1996): códigos de correção de erros para viabilização da computação quântica na presença de ruído;
- Teorema de Holevo-Schumacher-Westmoreland (1997/98): minorante da capacidade de canal quântico na presença de ruído;  
Teorema de Lloyd-Shor-Devetak (2005): 2o. teorema de Shannon para canais quânticos.
- Algoritmo de Childs *et al* (2003): pesquisa em grafo;
- Modelos alternativos de computação quântica (XXI): equivalência entre circuitos, processos adiabáticos e processos irreversíveis.

### 3 Alguns desafios – vencidos e ainda por vencer

5

- **Computação quântica**

- Resolução (mais) eficiente de problemas:

- \* **Ganho exponencial**: pesquisa em grafo;

- \* **Factorização em primos polinomial**: **ganho exponencial?**

- \*  **$NP \subseteq BQP?$   $SAT \in BQP?$**

- Realização de computador quântico:

- \* **Memória**: até 7 qubits em laboratório...

- \* **Memórias maiores? Utilizáveis na prática?**

- **Informação quântica**

- Comunicação (mais) segura:

- \* **Segurança perfeita na partilha de chave**: fibra óptica até 122km;

- \* **Distâncias maiores? Via satélite?**



## 5 Investigação no IST

7

### Projecto

FEDER POCI/MAT/55796/2004 **QUANTLOG**

Janeiro 1, 2005 - Dezembro 31, 2007

<http://clc.math.ist.utl.pt/quantlog.html>

**CLC** / CFIF / CFP / CEMAT / CAMGSD (/ CEMAPRE / GFM)

### Seminário (quase) semanal

QCI: sextas-feiras 15h00 PG04.35 (desde 26/09/2003)

<http://sem.math.ist.utl.pt/qci/>

### Workshop

Lisbon Quantum Computation, Information and Logic (LQCIL'07)

IST, 18-20 de Julho de 2007

Organizadores: P. Mateus, C. Nunes e Y. Omar

<http://wslc.math.ist.utl.pt/lqcil07/>

- Física da computação e informação quânticas (com U College)
  - Entrelaçamento em sistemas de estado sólido.
- Algoritmos quânticos (com U Waterloo)
  - Pesquisa quântica de padrões genómicos (*NATO ASI*);
  - Comparação entre passeios aleatórios e passeios quânticos;
  - Solução quântica para *SAT* (gap problem).
- Autómatos quânticos (com Tsinghua U)
  - Minimização do número de qubits;
  - Composição e interconexão.

- **Lógica quântica exógena** (QL Handbook com Kings College et al)
  - Valoração quântica = sobreposição de valorações clássicas;
  - Axiomatização completa (*Information and Computation*);
  - Lógica de Hoare para programas quânticos.
- **Aplicações em segurança** (com U Berkeley e U Pennsylvania)
  - Composicionalidade de protocolos quânticos (*ENTCS*);
  - Ataques quânticos a protocolo clássico de sistema de prova sem transferência de conhecimento;
  - Protocolos quânticos para realização de contratos.

- Bit clássico (bit)

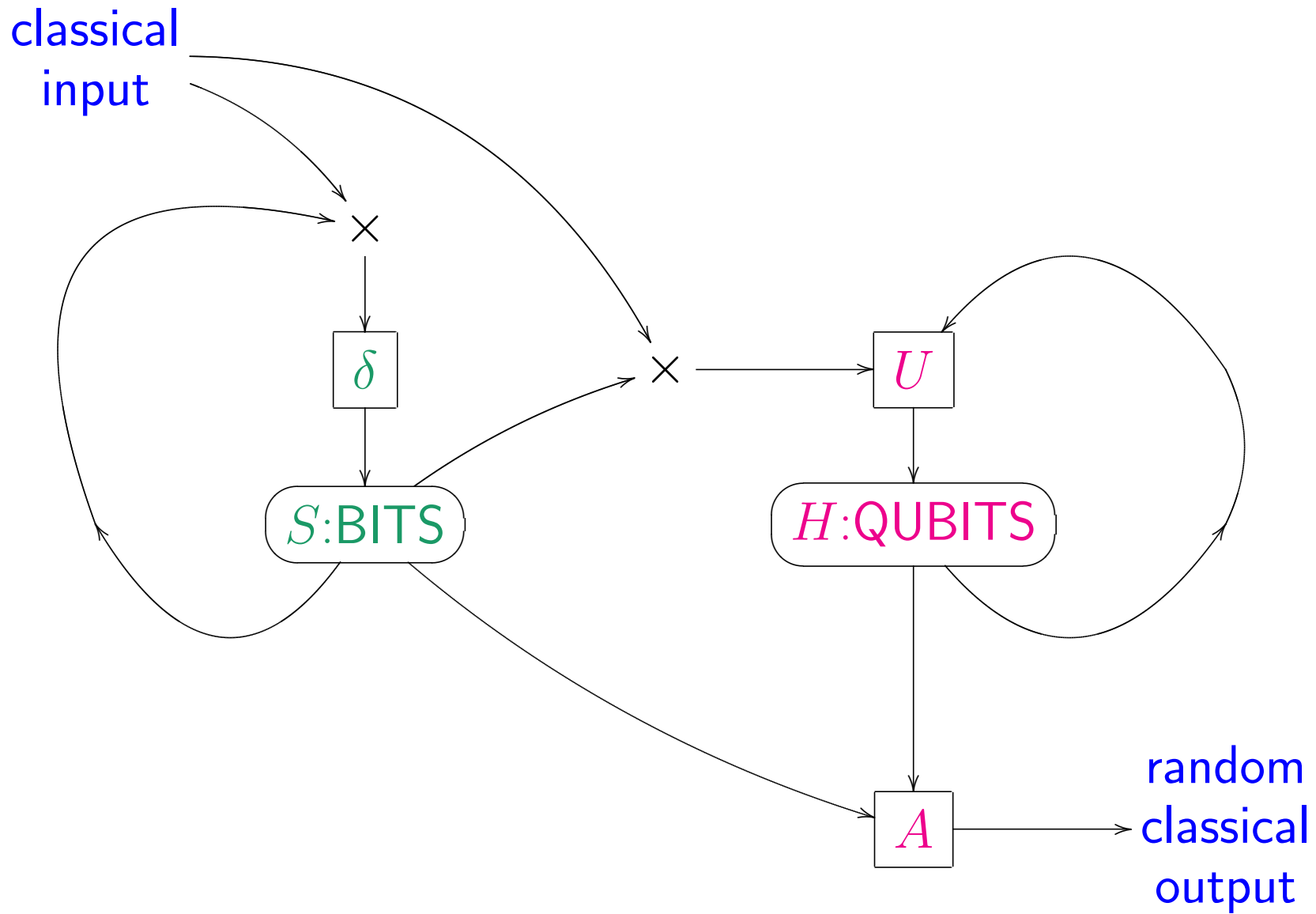
- Estados: *verdadeiro* ou *falso* ( $|1\rangle$  ou  $|0\rangle$ );
- “Gato vivo?": verdadeiro ou falso.

- Bit quântico (qubit)

- Espaço de estados: espaço de Hilbert de dimensão 2;
- Estado = sobreposição unitária de estados clássicos =  $\alpha|1\rangle + \beta|0\rangle$ ;
- “Gato vivo?": sobreposição de verdadeiro e falso.

- Sistema quântico

- Estados = vectores unitários do espaço de Hilbert em causa;
- Transições = transformações unitárias;
- Medições recorrendo a observáveis com resultados aleatórios: os resultados possíveis são os elementos do espectro.



- Pretende-se **minimizar** a dimensão de  $H$  (i.e. **número de qubits**).
- Eventual aumento do cardinal de  $S$  (i.e. número de bits)...
- Mas, **o aumento do número de bits não deve ser exponencial face à diminuição no número de qubits!**
- Caso contrário, é sempre possível eliminar completamente a componente quântica...
- **Algoritmo de optimização?**
- Minimização concomitante da parte clássica?
- Extensão dos resultados a outras noções mais gerais de autómato quântico?
- Nomeadamente, permitindo saídas quânticas e misturas...