Computação Quântica: Complexidade e Algoritmos

Carlos H. Cardonha

Marcel K. de Carli Silva

Cristina G. Fernandes (orientadora)

Departamento de Ciência da Computação

Instituto de Matemática e Estatística

Universidade de São Paulo

Apoio financeiro FAPESP (03/13236-0 e 03/13237-7)

Visão Geral

O que é?
Explorar efeitos quânticos para acelerar computações

Motivação
Evidências de maior poder computacional

Assuntos estudados

- Fatoração eficiente de inteiros,
  podendo quebrar o RSA
- Complexidade Computacional no modelo quântico

Pré-requisitos

- Espaços de Hilbert
  (Álgebra Linear sobre complexos)
- Regras do jogo no modelo quântico
  (superposição de valores)
- Máquinas de Turing no modelo clássico
- Computação Reversível no modelo clássico

Algoritmos

- Algoritmos de Deutsch, Deutsch-Jozsa e Simon:
  problemas "artificiais" que evidenciam o
  maior poder computacional do modelo quântico

- Algoritmo de Shor:
  fatoração de inteiros em tempo polinomial

- Algoritmo de Grover:
  busca numa seqüência qualquer em $O(\sqrt{n})$

Complexidade

- Máquinas de Turing quânticas:
  superposição de configurações
  mais restrições na construção
  paralelismo exponencial nas computações

- Máquina de Turing quântica universal:
  simula eficientemente a execução de
  qualquer máquina de Turing quântica

- Classes de Complexidade Clássicas e Quânticas:
  Relação entre as principais classes
  (incluindo probabilísticas)

Conclusão

- aprender a escrever textos matemáticos
- capacidade de comunicação com a orientadora
- contato com o ambiente acadêmico
- decifrar artigos mal escritos
- trabalhar com prazos inadiáveis
- Jornadas de Iniciação Científica no IMPA
- realizar seminários

Fim

Sítio:
`http://www.linux.ime.usp.br/~magal/quantum/`

Carlos: `cardonha@ime.usp.br`

Marcel: `magal@ime.usp.br`

Cristina (orientadora): `cris@ime.usp.br`