A Revolução da Computação Quântica:
progressos recentes e expectativas

Introdução a ECI – 2019/1

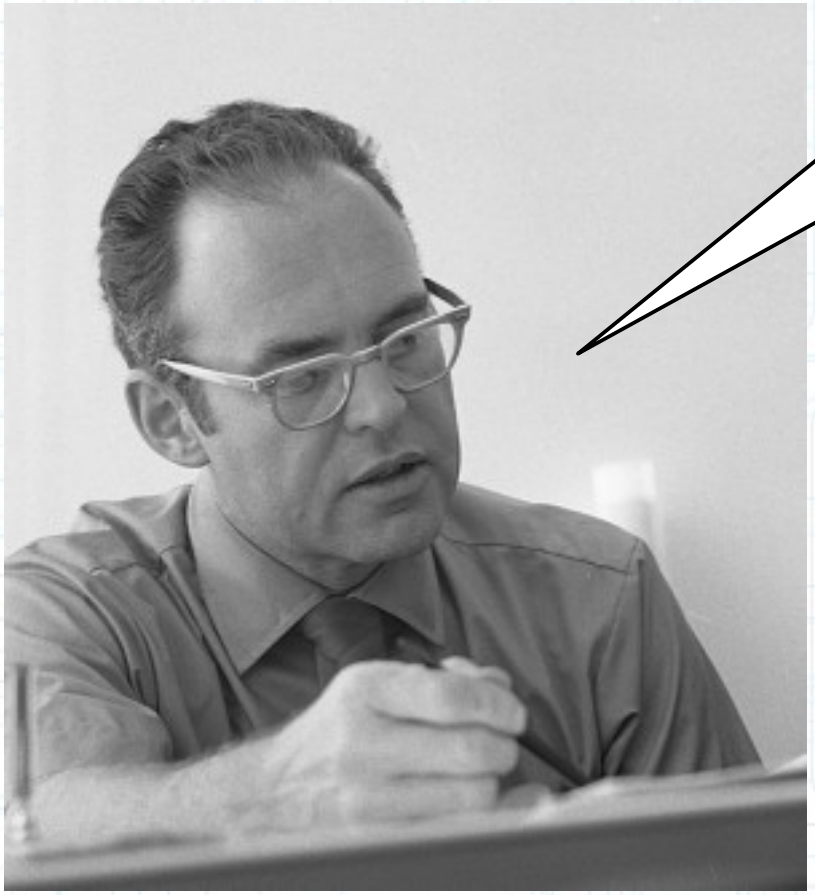
Franklin Marquezino
franklin@cos.ufrj.br

Agenda

- O que é a computação quântica
- Como são os computadores quânticos
- O que é possível fazer com um computador quântico
- Alguns problemas interessantes para pesquisa
- O que é necessário para ingressar nessa área

O que é a computação quântica

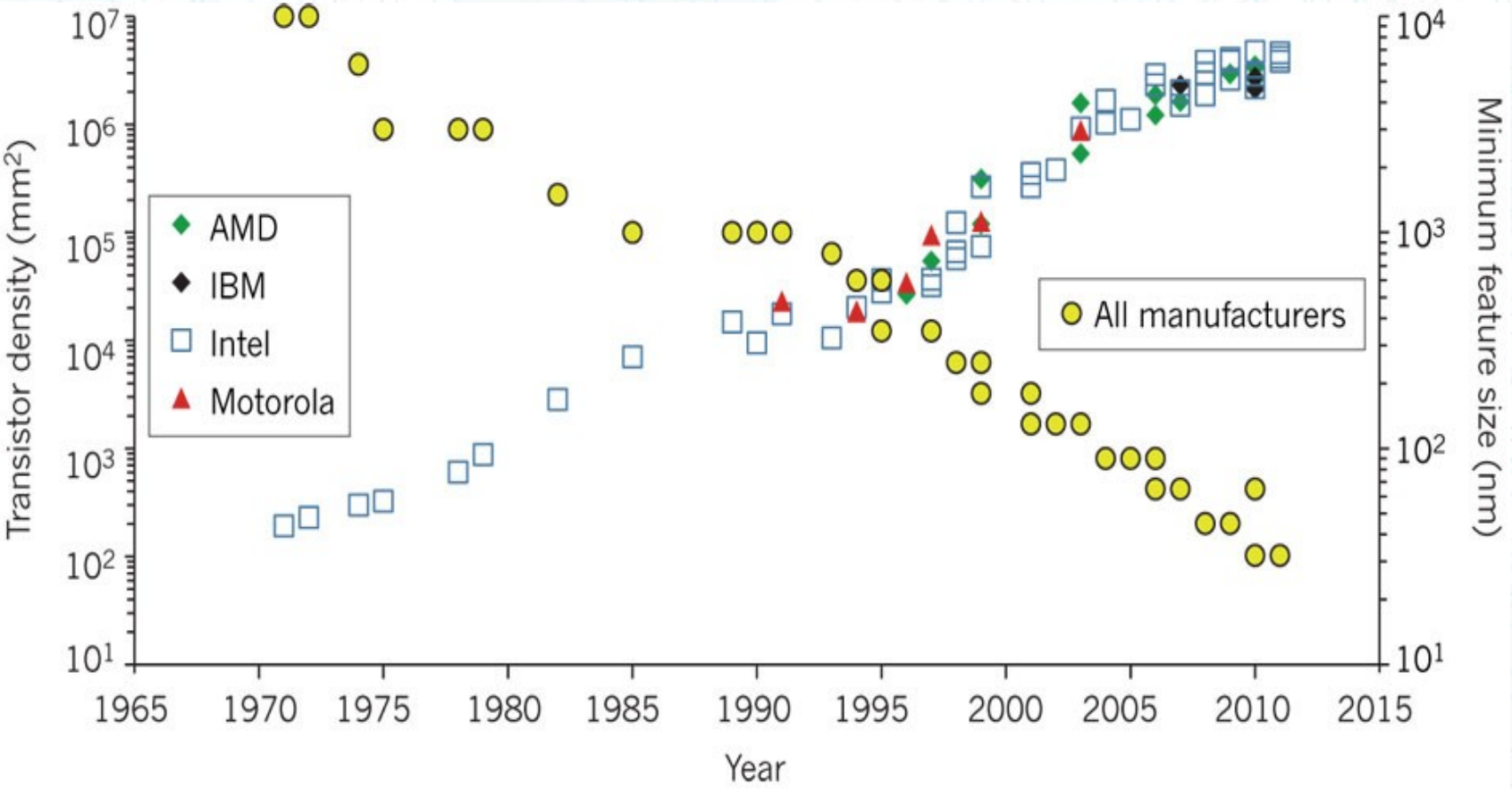
A famosa lei de Moore



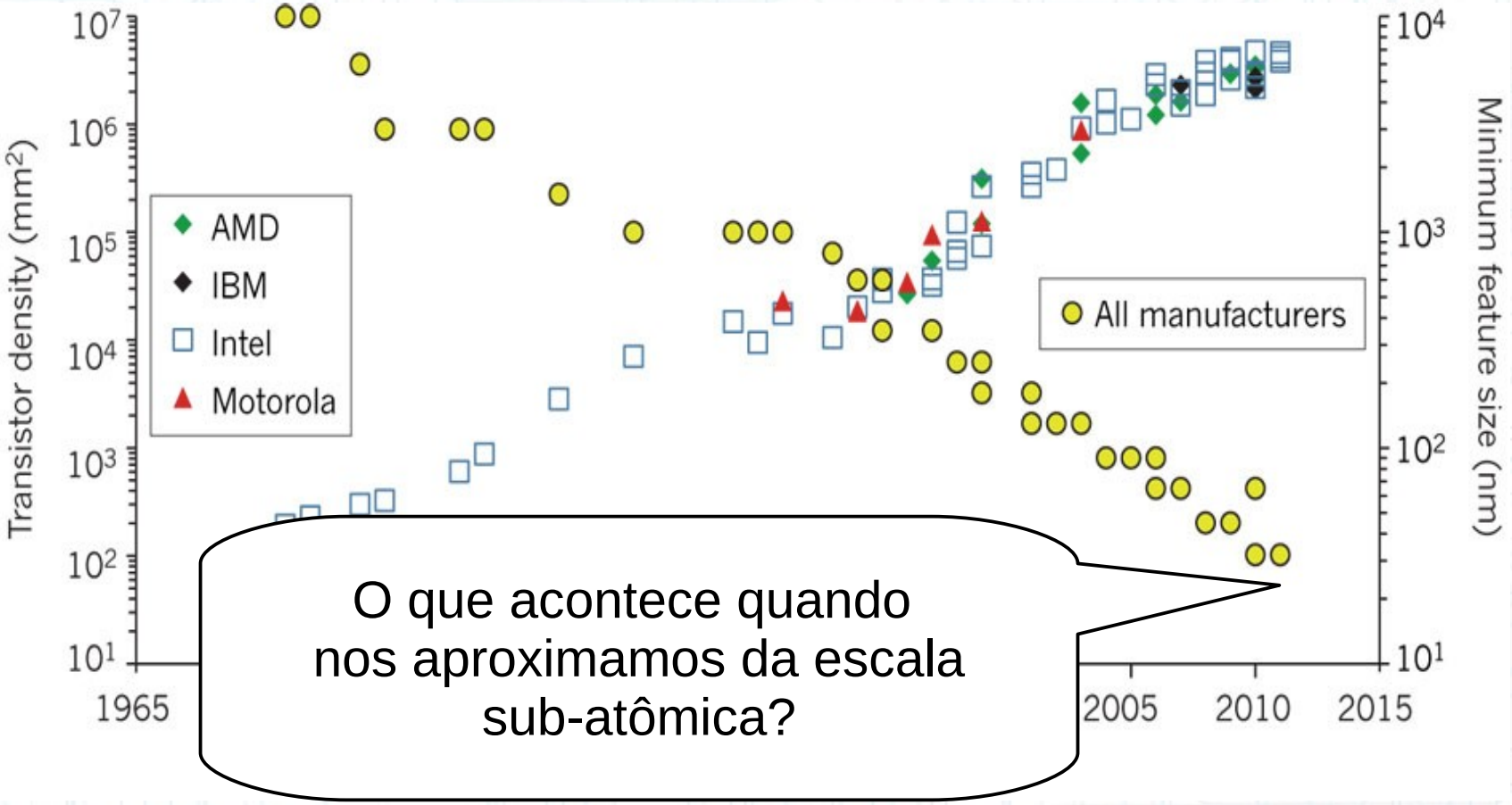
O número de transistores por chip vai dobrar aproximadamente a cada 18 meses

(Gordon Moore, 1965)

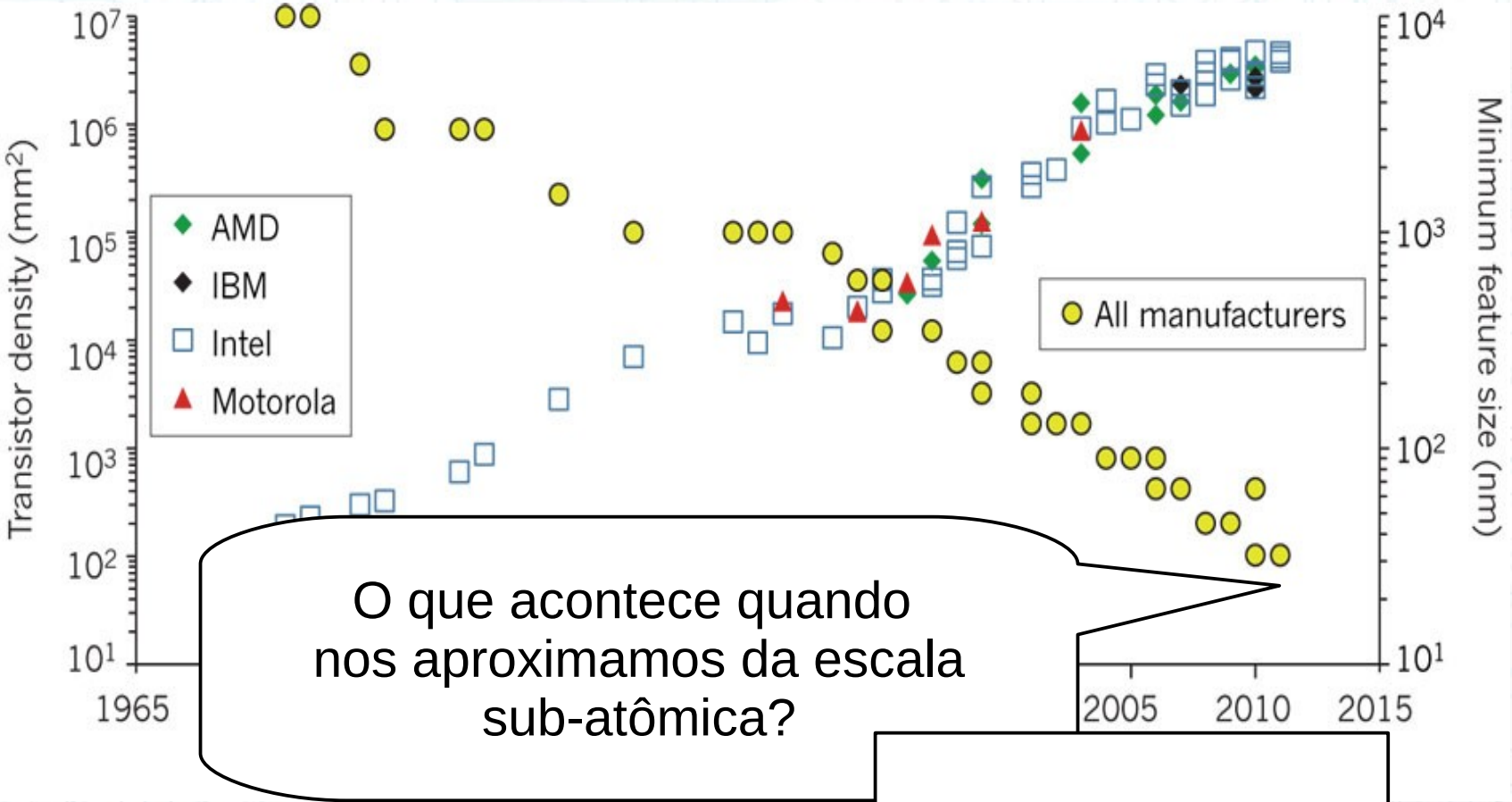
A famosa lei de Moore



A famosa lei de Moore



A famosa lei de Moore

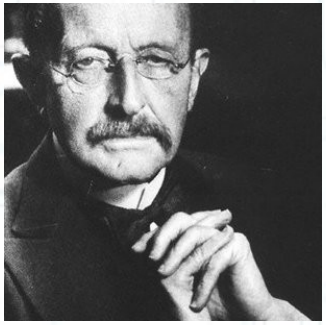


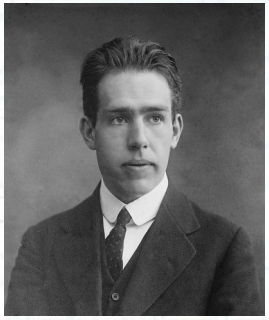
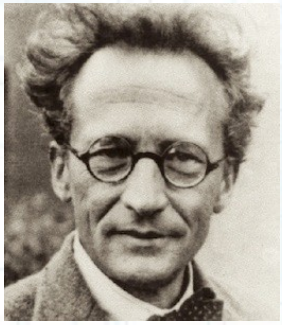
O que acontece quando nos aproximamos da escala sub-atômica?

Mecânica Quântica!

A revolução da física moderna

- Mecânica clássica: funciona muito bem para descrever sistemas macroscópios
- Entretanto… quando consideramos dimensões muito pequenas ou velocidades muito próximas à da luz… falha!
- Partículas muito pequenas: **Mecânica Quântica**
- Velocidades muito altas: Teoria da Relatividade

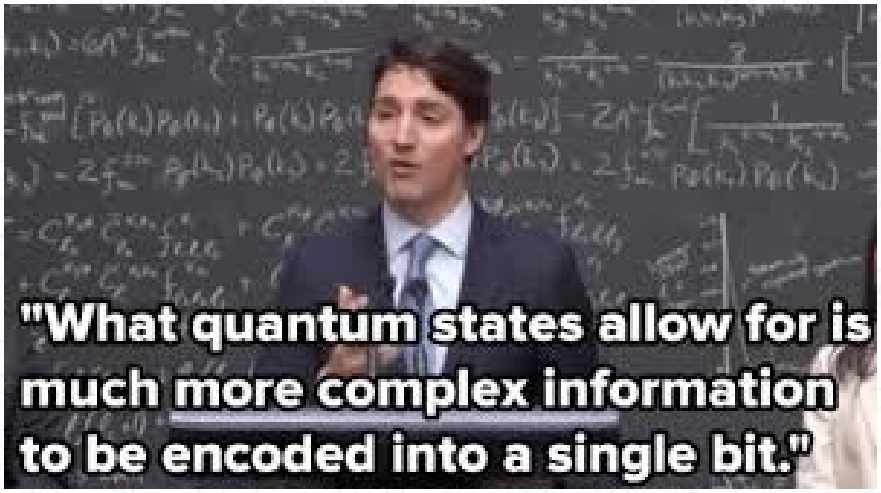




O que é essa mecânica quântica, afinal?

- MQ: pode ser muito difícil, dependendo da abordagem que você usa para aprender
- Dica: a computação quântica é uma excelente abordagem para aprender MQ!

O que é essa mecânica quântica, afinal?

- MQ: pode ser muito difícil, dependendo da abordagem que você usa para aprender
- Dica: a computação quântica é uma excelente abordagem para aprender MQ!

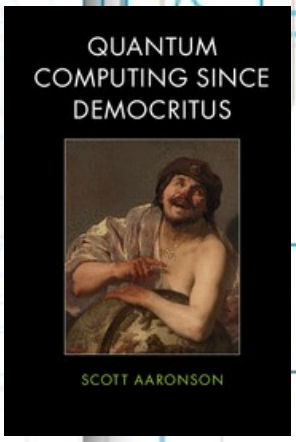


O que é essa mecânica quântica, afinal?

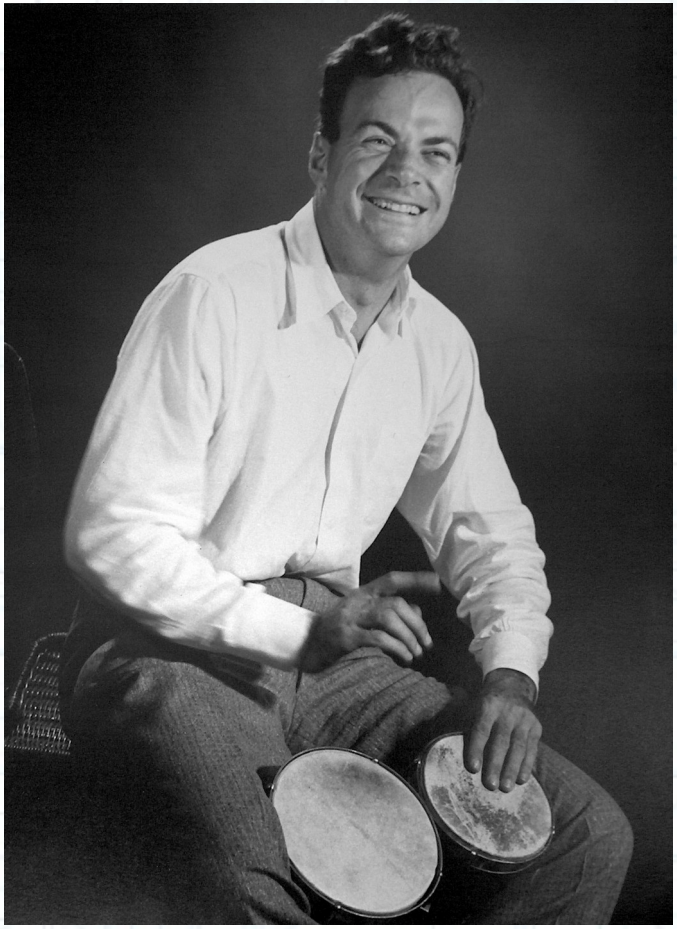
- MQ: pode ser muito difícil, dependendo da abordagem que você usa para aprender
- Dica: a computação quântica é uma excelente abordagem para aprender MQ!
- Podemos resumir as “regras do jogo”:
  - Postulado I: como represento um estado quântico
  - Postulado II: como esse estado evolui
  - Postulado III: como compor estados maiores
  - Postulado IV: como fazer uma leitura desse estado

O que é essa mecânica quântica, afinal?

- MQ: pode ser muito difícil, dependendo da abordagem que você usa para aprender
- Dica: a computação quântica é uma excelente abordagem para aprender MQ!
- Podemos resumir as “regras do jogo”:
  - Postulado I: como represento um estado quântico
  - Postulado II: como esse estado evolui
  - Postulado III: como compor estados maiores
  - Postulado IV: como fazer uma leitura desse estado
- Dica de leitura: *Quantum Computing since Democritus*, de Scott Aaronson



Física e Computadores



Richard Feynman

- Os nossos computadores são eficientes para simular Mecânica Quântica?
- “Simulating physics with computers”, 1982
- E se o computador for construído usando a própria Mecânica Quântica?

Então, o que é a computação quântica?

- Aplicação dos postulados da Mecânica Quântica para desenvolver um novo modelo de computação
- Por quê precisamos nos preocupar com isso?

Então, o que é a computação quântica?

- Aplicação dos postulados da Mecânica Quântica para desenvolver um novo modelo de computação
- Por quê precisamos nos preocupar com isso?
  - Simulação eficiente de sistemas quânticos, algoritmos mais rápidos, criptografia mais segura, resultados teóricos interessantes, etc

Como são os computadores quânticos

Como funciona um computador quântico?

- Na computação clássica: bits

$|0\rangle$ ou $|1\rangle$

Como funciona um computador quântico?

- Na computação clássica: bits

|0> ou |1>

Notação de Dirac
(é um pouco diferente, sim!)

Como funciona um computador quântico?

- Na computação clássica: bits

|0> ou |1>

- Na computação clássica probabilística:

|0> ou |1>, sendo
|0> com probabilidade p,
|1> com probabilidade 1-p

Como funciona um computador quântico?

- Na computação clássica: bits

$|0\rangle$ ou $|1\rangle$

- Na computação clássica probabilística:

$|0\rangle$ ou $|1\rangle$, sendo
$|0\rangle$ com probabilidade p,
$|1\rangle$ com probabilidade 1-p

Tem que ser um número real entre 0 e 1

Como funciona um computador quântico?

- Na computação clássica: bits

|0> ou |1>

- Na computação clássica probabilística:

|0> ou |1>, sendo
|0> com probabilidade p,
|1> com probabilidade 1-p

- Na computação quântica: **q-bits**, **qubits**
  - combinação linear a|0> + b|1>,

Como funciona um computador quântico?

- Na computação clássica: bits

|0> ou |1>

- Na computação clássica probabilística:

|0> ou |1>, sendo
|0> com probabilidade p,
|1> com probabilidade 1-p

- Na computação quântica: **q-bits**, **qubits**

combinação linear a|0> + b|1>,

Superposição!

Como funciona um computador quântico?

- Na computação clássica: bits

$|0\rangle$ ou $|1\rangle$

- Na computação clássica probabilística:

$|0\rangle$ ou $|1\rangle$, sendo
$|0\rangle$ com probabilidade p,
$|1\rangle$ com probabilidade 1-p

- Na computação quântica: **q-bits**, **qubits**

combinação linear $a|0\rangle + b|1\rangle$,
$|0\rangle$ com **amplitude** a,
$|1\rangle$ com **amplitude** b,
$|a|^2 + |b|^2 = 1$

Número complexo!
Parte real e parte imaginária!
Pode até ser negativo!

Sim, qubits. E daí?

- Superposição pode envolver vários qubits. Operações atuam em todos os valores da superposição ao mesmo tempo (**paralelismo quântico**)

Sim, qubits. E daí?

- Superposição pode envolver vários qubits. Operações atuam em todos os valores da superposição ao mesmo tempo (**paralelismo quântico**)
- Amplitudes negativas podem cancelar com amplitudes positivas, reforçando a resposta correta e suprimindo as respostas erradas! (**interferência**)

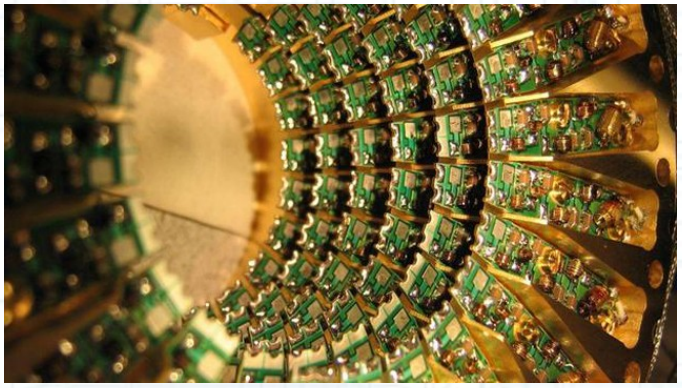
Sim, qubits. E daí?

- Superposição pode envolver vários qubits. Operações atuam em todos os valores da superposição ao mesmo tempo (**paralelismo quântico**)
- Amplitudes negativas podem cancelar com amplitudes positivas, reforçando a resposta correta e suprimindo as respostas erradas! (**interferência**)
- Algumas superposições especiais não tem análogo no mundo clássico (**emaranhamento**)

Sim, qubits. E daí?

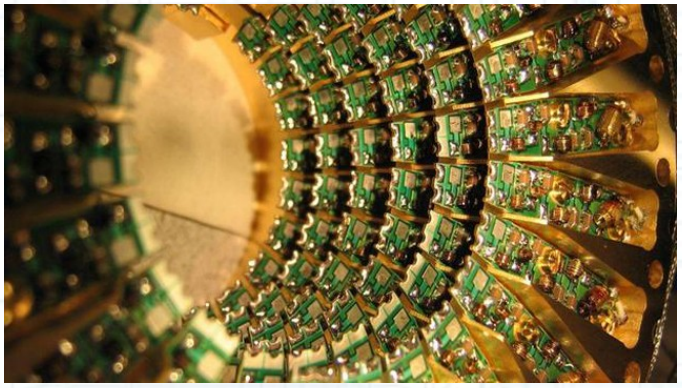
- Superposição pode envolver vários qubits. Operações atuam em todos os valores da superposição ao mesmo tempo (**paralelismo quântico**)
- Amplitudes negativas podem cancelar com amplitudes positivas, reforçando a resposta correta e suprimindo as respostas erradas! (**interferência**)
- Algumas superposições especiais não tem análogo no mundo clássico (**emaranhamento**)
- Porém, **medições** (a leitura dos resultados) não são triviais… tem que ter cuidado!

Posso executar algoritmos quânticos no meu computador?



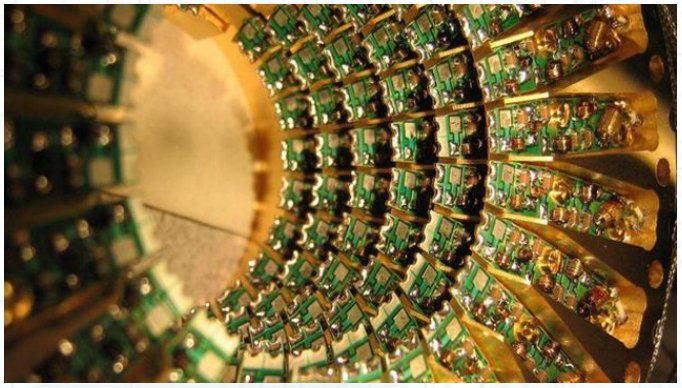
- NÃO pode!
- No máximo, você pode simular esses algoritmos, mas será MUITO lento!
- Para executar algoritmos quânticos de verdade, você precisa de um computador quântico

Posso executar algoritmos quânticos no meu computador?



- NÃO pode!
- No máximo, você pode simular esses algoritmos, mas será MUITO lento!
- Para executar algoritmos quânticos de verdade, você precisa de um computador quântico
  - IBM disponibiliza um computador quântico para qualquer um acessar na nuvem http://www.research.ibm.com/quantum/
  - Rigetti também: https://www.rigetti.com/

Posso executar algoritmos quânticos no meu computador?



- NÃO pode!
- No máximo, você pode simular esses algoritmos, mas será M
- Para executar algoritm
  verdade, você pre
  quântico

14 qubits disponível para todos
20 qubits mediante convite

  - IBM disponibiliza um computador quântico para qualquer um acessar na nuvem http://www.research.ibm.com/quantum/
  - Rigetti também: https://www.rigetti.com/

Posso executar algoritmos quânticos no meu computador?

- NÃO pode!
- No máximo, você po… algoritmos, mas ser…
- Para executar alg… verdade, você pr… quântico
  - IBM disp…nibiliza um computador quântico para qualquer um acessar na nuvem http://www.research.ibm.com/quantum/
  - Rigetti também: https://www.rigetti.com/

26 qubits em simulação
19 qubits reais mediante convite
(rodar simulações antes de requisitar)

14 qubits disponível para todos
20 qubits mediante convite

Como programar um computador quântico

- Vocês podem começar hoje mesmo:
  - Abram uma conta no IBM Quantum Experience e façam o tutorial
  - Em breve, vejam meu material em http://www.github.com/programaquantica

Como programar um computador quântico

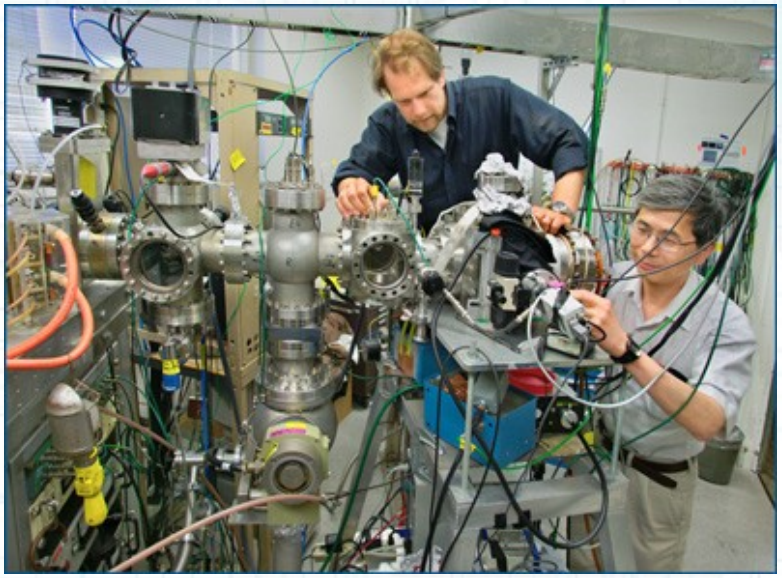
- Vocês podem começar hoje mesmo:
  - Abram uma conta no IBM Quantum Experience e façam o tutorial
  - Em breve, vejam meu material em http://www.github.com/programaquantica
- Possibilidades atuais:
  - IBM: circuitos, QASM, QISKit (em Python)
  - Rigetti: Forest (em Python)
  - D-Wave: C, C++, Python, Matlab
  - Diversas plataformas: Microsoft Q#, ProjectQ

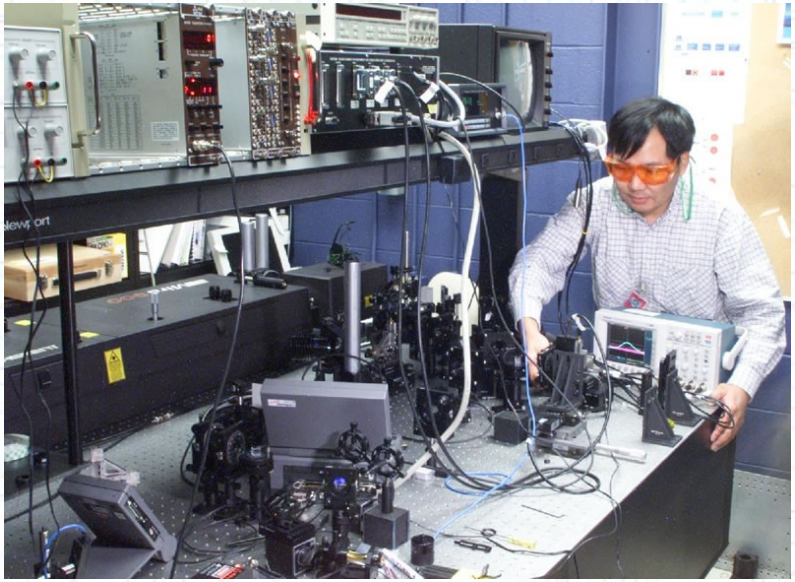
Como programar um computador quântico

- Vocês podem começar hoje mesmo:
  - Abram uma conta no IBM Quantum Experience e façam o tutorial
  - Em breve, vejam meu material em http://www.github.com/programaquantica
- Possibilidades at
  - IBM: circuit
  - Rigetti: Forest ... Python)
  - D-Wave: C, C++, Python, Matlab
  - Diversas plataformas: Microsoft Q#, ProjectQ

D-Wave: precisa antes converter problema original em um problema QUBO (quadratic unconstrained binary optimization)

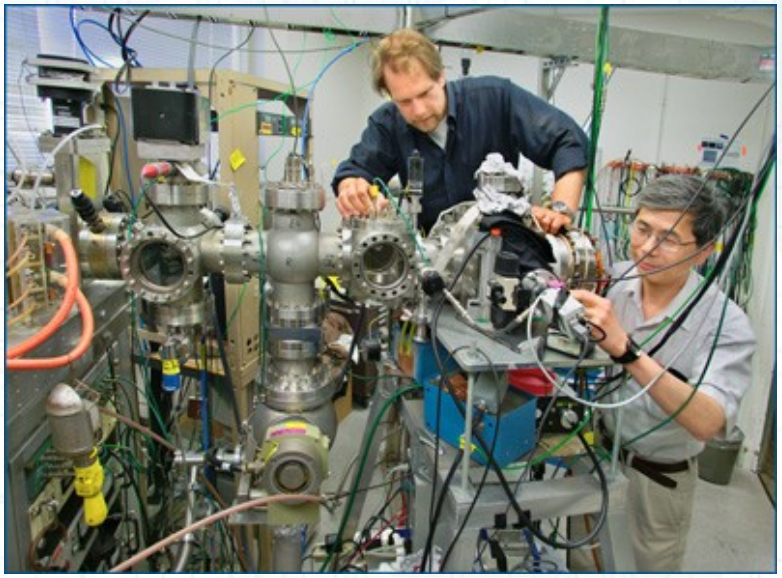
Hardware quântico

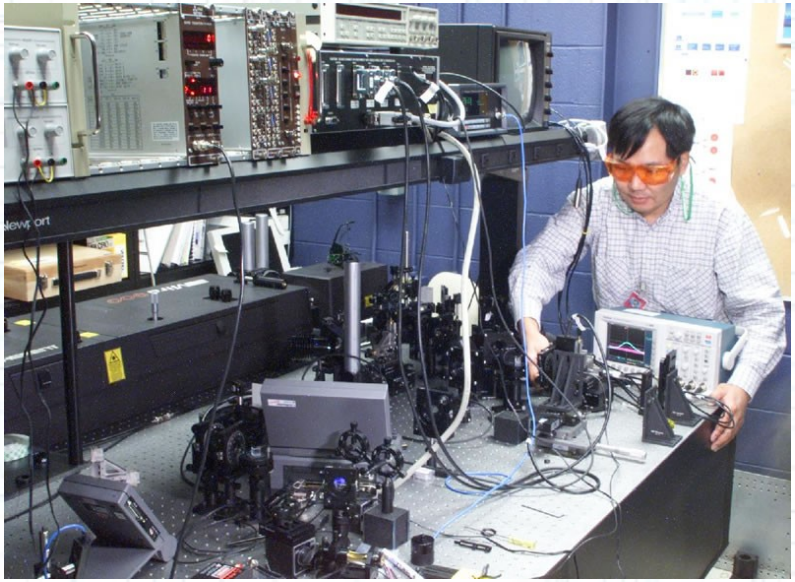




- Grande desafio tecnológico…
- Difícil isolar e manipular muitas partículas quânticas por tempo suficiente…

Hardware quântico





- Grande desafio tecnológico…
- Difícil isolar e manipular muitas partículas quânticas por tempo suficiente…
- PORÉM, grandes avanços recentes!

Hardware quântico

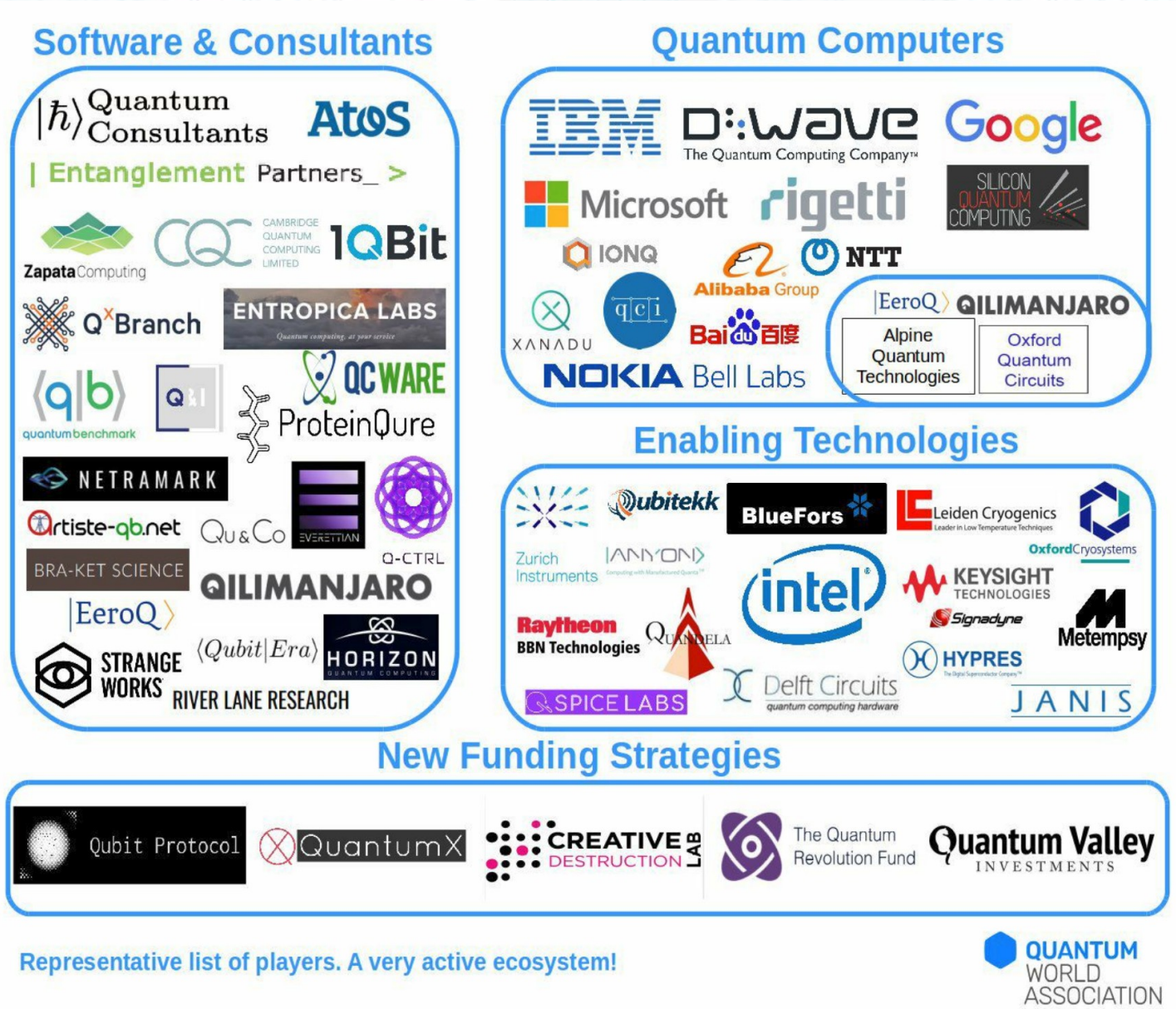
- Maior simulação já realizada:
  - Universidade de Melbourne, 60 qubits
  - Antes: IBM, 56 qubits

Hardware quântico

- Maior simulação já realizada:
  - Universidade de Melbourne, 60 qubits
  - Antes: IBM, 56 qubits
- Computadores quânticos hoje:
  - IBM: 20 qubits, 50 qubits(?)
  - Rigetti: 19 qubits, 128 qubits(?)
  - Google: 72 qubits(?)
  - Intel: 49 qubits(?)

(?) : anunciado

Empresas na CQ



Representative list of players. A very active ecosystem!

QUANTUM WORLD ASSOCIATION

O que é possível fazer com um computador quântico

O que vamos poder fazer com um computador quântico?

- Possíveis aplicações incluem
  - criptoanálise,
  - desenvolvimento de fármacos e materiais,
  - aprendizado de máquina,
  - diversos problemas de otimização
  - etc
- Vejam, por exemplo:

http://www.research.ibm.com/quantum/expertise.html
http://www.dwavesys.com/quantum-computing/applications

O que vamos poder fazer com um computador quântico?

- Os algoritmos mais famosos:
  - Shor, fatoração de inteiros, 1994
  - Grover, busca não-ordenada, 1996
  - Algoritmo adiabático, 2000
  - HHL, sistemas lineares, 2008
  - QAOA, otimização, 2014

Já temos muitos algoritmos importantes!

- Vejam a lista atualizada em http://math.nist.gov/quantum/zoo/

- ***Factoring, Discrete-log, Pell's Equation, Principal Ideal, Unit Group, Class Group***, ***Gauss Sums,*** *Solving Exponential Congruences,* ***Matrix Elements of Group Representations***, *Verifying Matrix Products, Subset-sum, Searching,* ***Abelian Hidden Subgroup, (Some) Non-Abelian Hidden Subgroup***, *Bernstein-Vazirani,* ***Deutsch-Jozsa***, *Formula Evaluation, Gradients, Structured Search, and Learning Polynomials,* ***Hidden Shift, Pattern matching, Linear Systems***, *Ordered Search, Graph Properties in the Adjacency Matrix Model, Graph Properties in the Adjacency List Model,* ***Welded Tree***, *Collision Finding and Element Distinctness, Graph Collision, Matrix Commutativity, Group Commutativity,* ***Hidden Nonlinear Structures***, *Center of Radial Function,* ***Group Order and Membership, Group Isomorphism***, *Statistical Difference,* ***Finite Rings and Ideals***, *Counterfeit Coins, Matrix Rank, Matrix Multiplication over Semirings, Subset finding, Search with Wildcards, Network flows,* ***Electrical Resistance***, ***Quantum Simulation, Knot Invariants, Three-manifold Invariants, Partition Functions***, *Adiabatic Algorithms,* ***Zeta Functions, Weight Enumerators,*** *Simulated Annealing,* ***String Rewriting, Matrix Powers***

Criptografia quântica avançando a passos largos!

- Tudo começou em 1970/1983: dinheiro quântico!
- Distribuição quântica de chaves
  - Chaves seguras, invioláveis
  - Permite que se use cifra de Vernam
  - Disponível comercialmente!

Alguns problemas interessantes para pesquisa

Áreas interessantes

- Desenvolvimento de novos algoritmos
  - Aplicação de técnicas conhecidas
  - Desenvolvimento de novas técnicas

Áreas interessantes

- Desenvolvimento de novos algoritmos
  - Aplicação de técnicas conhecidas
  - Desenvolvimento de novas técnicas
- Passeios quânticos
  - Desenvolvimento de novos algoritmos
  - Relações com Teoria de Grafos, Redes Complexas etc, análises de aspectos físicos etc.

Áreas interessantes

- Desenvolvimento de novos algoritmos
  - Aplicação de técnicas conhecidas
  - Desenvolvimento de novas técnicas
- Passeios quânticos
  - Desenvolvimento de novos algoritmos
  - Relações com Teoria de Grafos, Redes Complexas etc, análises de aspectos físicos etc.
- Simulação de algoritmos quânticos por computadores clássicos

Áreas interessantes

- Desenvolvimento de novos algoritmos
  - Aplicação de técnicas conhecidas
  - Desenvolvimento de novas técnicas
- Passeios quânticos
  - Desenvolvimento de novos algoritmos
  - Relações com Teoria de Grafos, Redes Complexas etc, análises de aspectos físicos etc.
- Simulação de algoritmos quânticos por computadores clássicos
- Demonstração de resultados teóricos

Áreas interessantes

- Desenvolvimento de novos algoritmos
  - Aplicação de técnicas conhecidas
  - Desenvolvimento de novas técnicas
- Passeios quânticos
  - Desenvolvimento de novos algoritmos
  - Relações com Teoria de Grafos, Redes Complexas etc, análises de aspectos físicos etc.
- Simulação de algoritmos quânticos por computadores clássicos
- Demonstração de resultados teóricos
- Implementações físicas

O que é necessário para ingressar nessa área

Como ingressar nessa área?

- **Computação:**
  diversas disciplinas sobre algoritmos, complexidade, estruturas de dados, grafos, otimização etc
- **Álgebra Linear**:
  nos números complexos, e com uma notação ligeiramente diferente
- **Mecânica Quântica**:
  resumida em 4 postulados
  - Importante: **não** precisa ser físico!

Como ingressar nessa área?

- Iniciação Científica
  - COPPE/PESC
  - Às vezes surgem bolsas PIBIC, fiquem atentos!
  - Se tiverem interesse, escrevam email!
- Mestrado, doutorado:
  - COPPE/PESC (CAPES 7)
  - Duas disciplinas por ano: Introdução à Computação Quântica, Caminhadas Quânticas e Algoritmos
  - Alunos ouvintes são bem-vindos
  - LNCC, UFRJ/IF, CBPF etc.
- Seminários
  - COPPE/PESC, Grupo de Grafos

Perguntas?

Vejam também:
http://www.cos.ufrj.br/~franklin

ou escrevam para:
franklin@cos.ufrj.br