Computação Quântica
Aula 01

Murilo V. G. da Silva

Departamento de Informática
Universidade Federal do Paraná

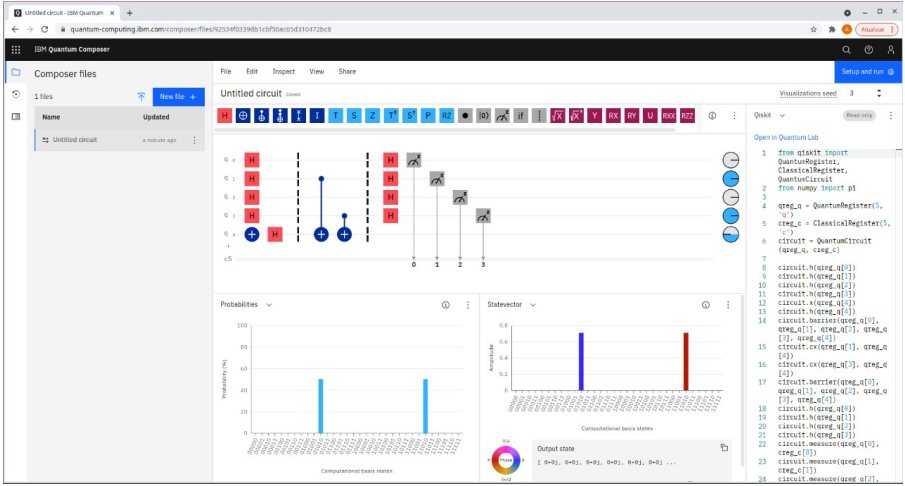
08/08/2023

Disciplina de Computação Quântica

- Página da disciplina centraliza informações relevantes
- Aulas presenciais (vídeos opcionais)
- Curso dividido em duas partes:
  - 1. Base matemática
  - 2. Algoritmos

Disciplina de Computação Quântica

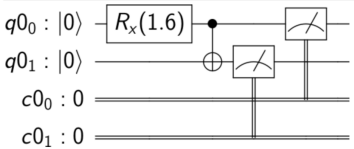
- Aulas "experimentais"



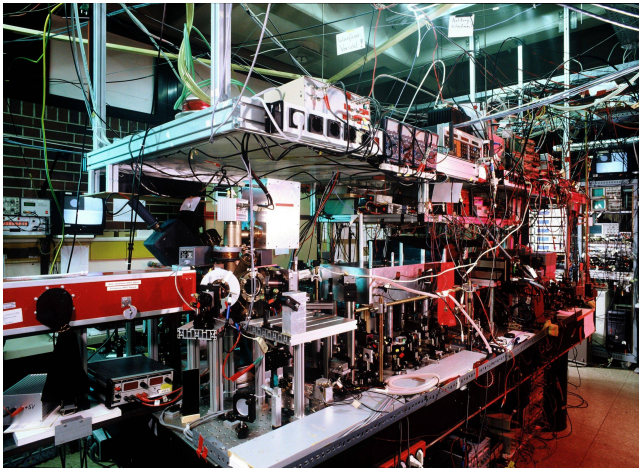
Computação Quântica: (1) Realidade comercial?

In [7]:
```
from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
from qiskit.tools.visualization import circuit_drawer
import numpy as np

qr = QuantumRegister(2)
cr = ClassicalRegister(2)
qp = QuantumCircuit(qr,cr)

qp.rx( np.pi/2,qr[0])
qp.cx(qr[0],qr[1])

qp.measure(qr,cr)

circuit_drawer(qp)
```

Out[7]:



Computação Quântica: (2) Pesquisa científica?



Laboratório de Computação Quântica, Universidade de Innsbruck.

Computação Quântica: (3) É pra valer isso?

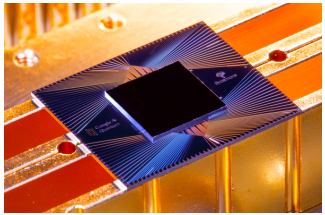
Leonid Levin: "Quantum computing **must** be impossible!"

Posição Atual

Atual posição científica (comumente aceita):

- Teoria: Computação quântica **tem** que ser possível
- Prática: Computadores quânticos existentes ainda não são **universais** e **escaláveis**
  Estamos na Era NISQ

  Supremacia quântica iminente/atingida (?)

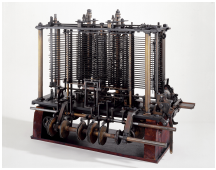
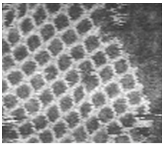
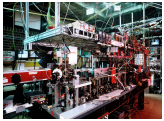


- Teremos uma aula para discutir isso

Teoria da Computação em 6 slides

(algoritmos, computadores, modelos matemáticos, modelos fisicamente realizáveis)

Computação ocorrendo em diferentes substratos físicos: circuitos eletrônicos, engrenagens, DNA, partículas subatômicas:

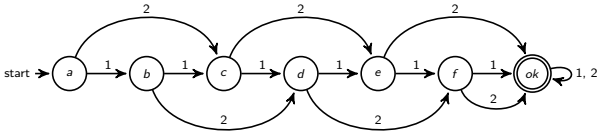




Computadores

Uma maneira de instanciar objetos abstratos e os **possíveis relacionamentos matemáticos** destes objetos abstratos em objetos físicos e o e os **possíveis graus de movimentos** destes objetos físicos.

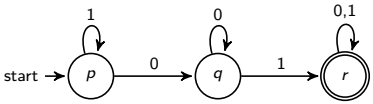
Pergunta Crucial: O meio físico faz diferença?

Objeto físico e modelo matemático:



- Uma máquina de vender chocolates é descrita por um DFA $D = (Q, \Sigma, \delta, q_0, F)$.
- Vamos esquecer o mundo físico por um instante...

Revisão de Teoria da Computação (modelos matemáticos)



- Definição matemática do diagrama acima: $D = (\{p, q, r\}, \{0, 1\}, \delta, q_0, \{q_2\})$ tal que $\delta(p, 1) = p$, $\delta(p, 0) = q$, $\delta(q, 0) = q$, $\delta(q, 1) = r$, $\delta(r, 0) = r$, $\delta(r, 1) = r$.
- Problemas que **NÃO** podem ser resolvidos por DFAs: e.g., palíndromos, primalidade, etc
- Problemas que **NÃO** podem ser resolvidos por PDAs: e.g., primalidade, etc

- Máquinas de Turing: Resolvem todos problemas algorítmicos

Revisão de Teoria da Computação (modelos matemáticos)

Teorema

Os seguintes **modelos matemáticos** são equivalentes:

- Máquina de Turing (MTs)
- Máquinas RAM abstratas
- Linguagem C
- Modelo aTAM (DNA)
- Circuitos Quânticos

Tese de Church-Turing

Funções computáveis por dispositivos fisicamente realizáveis = funções computáveis por MTs

Em outras palavras, a tese afirma que o meio físico não faz diferença em termos de computabilidade!

Complexidade Computacional entra na jogada

Teorema

Modelos matemáticos polinomialmente equivalentes:

- Máquina de Turing
- Máquinas RAM abstratas
- Linguagem C
- Modelo aTAM (DNA)

e.g., dado um certo problema computacional,

- Se existe um programa em C cuja execução resolva uma instância de tamanho n em $f(n)$ passos, então existe uma MT que resolve o mesmo problema em $O(f(n)^c)$ passos (c constante).
- Se existe uma MT que resolve uma instância de tamanho n em $f(n)$ passos, então existe um programa em C que resolve o mesmo problema em $O(f(n)^c)$ (c constante).
- Se existe uma "programa em aTAM" que resolva uma instância de tamanho n em $f(n)$ "passos", então existe um programa para Máquinas RAM abstratas em $O(f(n)^d)$ passos (c para uma constante).
- etc...

Complexidade Computacional entra na jogada

Teorema

Modelos matemáticos polinomialmente equivalentes:

- Máquina de Turing
- Máquinas RAM abstratas
- Linguagem C
- Modelo aTAM (DNA)

- Circuitos Quânticos (?)

Existem problemas para os quais algoritmos quânticos são **exponencialmente** mais rápidos que algoritmos clássicos conhecidos.

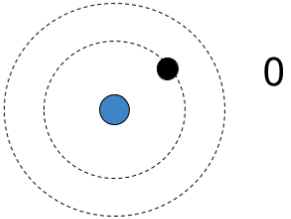
No nível mais fundamental da natureza o meio físico parece fazer diferença na eficiência da computação de alguns problemas

Mecânica Quântica 101

"Teoria da probabilidade com números complexos"

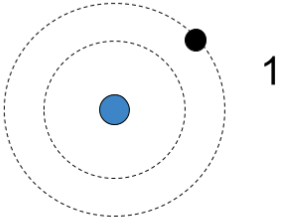
Átomos e bits

Um átomo segundo um teórico da computação:



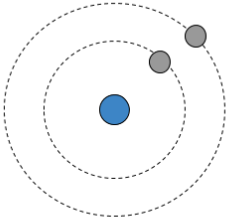
Átomos e bits

Um átomo segundo um teórico da computação:



Modelo probabilístico

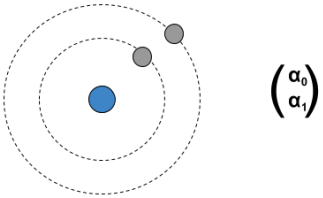
Supondo que haja incerteza no sistema:



0 ou 1 ?

Modelo probabilístico

Objeto físico (átomo) $\Leftrightarrow$ Modelo matemático (vetor em $\mathbb{R}^2$)



Exemplo de vetores descrevendo o sistema:

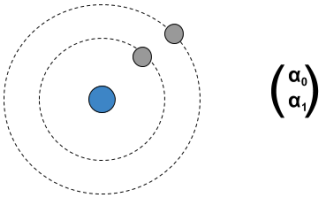
- $\begin{pmatrix} 0.3 \\ 0.7 \end{pmatrix}$ $\begin{pmatrix} 0.5 \\ 0.5 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Atenção: descrição do sistema $\neq$ bit obtido ao observarmos o sistema

Exemplos de bits observados:

- 1 1 1 0

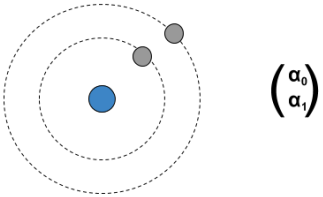
Probabilidade *vs* Mecânica Quântica



Modelo probabilístico:

- α_0, α_1 reais entre 0 e 1
- $\alpha_0 + \alpha_1 = 1$.
- Na "realidade" o objeto está no estado 0 ou 1
- Output: 0 ou 1

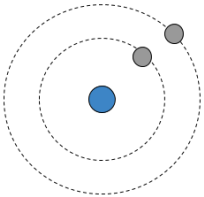
Probabilidade *vs* Mecânica Quântica



Mecânica quântica:

- α_0, α_1 complexos (possivelmente negativos)
- $|\alpha_0|^2 + |\alpha_1|^2 = 1$
- Não faz sentido dizer se objeto está no estado 0 ou 1 (interpretação comum)
- Output: 0 ou 1 (com probabilidade $|\alpha_0|^2$ ou $|\alpha_1|^2$ resp.)

Usando mecânica quântica para implementar "qubits"

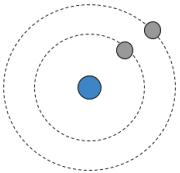


$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

Estado quântico descrito por números complexos

- O *estado quântico* de um objeto que pode assumir dois *estados* é descrito por um vetor com dois números complexos α_0 e α_1.
- Os valores α_0 e α_1 são chamados de amplitudes, sendo que $|\alpha_0|^2 + |\alpha_1|^2 = 1$.
- Ao medir o objeto, a probabilidade de observarmos o estado i é $|\alpha_i|^2$.

Usando mecânica quântica para implementar "qubits"



$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$

Note que: $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \boldsymbol{\alpha_0 |0\rangle + \alpha_1 |1\rangle}$

Obs: usaremos a notação $|0\rangle$ e $|1\rangle$ neste curso

Lembramos também que $|\alpha_0|^2 + |\alpha_1|^2 = 1, \quad \alpha_0, \alpha_1 \in \mathbb{C}$

O vetor $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ é chamado de qubit

Usando mecânica quântica para implementar "qubits"

Usando o spin de um elétron para registrar informação: **mesmo modelo matemático**

$|0\rangle$

Usando mecânica quântica para implementar "qubits"

Usando o spin de um elétron para registrar informação: **mesmo modelo matemático**

$|1\rangle$

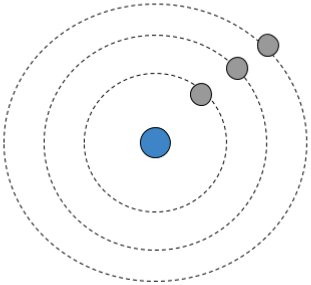
Usando mecânica quântica para implementar "qubits"

Usando o spin de um elétron para registrar informação: **mesmo modelo matemático**

$$|\Psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

As leis da mecânica quântica são as mesmas
(estado do átomo, spin de eletron, polarização de fotons, etc)

Usando mecânica quântica para implementar "qutrits"



$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{pmatrix}$$

$$|\Psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{pmatrix} = \alpha_0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \boldsymbol{\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle}$$

$$|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 = 1$$

Axioma da Sobreposição

Seja um sistema quântico que pode estar em k possíveis estados $|0\rangle, |1\rangle, ..., |k-1\rangle$

Axioma da Sobreposição: então o sistema pode estar em qualquer combinação linear dos estados:

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + ... + \alpha_{k-1} |k-1\rangle$$

$$\sum_{i=0}^{k-1} |\alpha_i|^2 = 1, \quad \alpha_i \in \mathbb{C}$$

Axioma da Sobreposição

Exemplo 1: para $k = 3$, um possível estado do sistema seria:

$$\frac{1}{\sqrt{3}}|0\rangle + \frac{i}{\sqrt{3}}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle$$

Exemplo 2: para $k = 4$, um possível estado do sistema seria:

$$\frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \left(\frac{1}{2} + \frac{i}{2}\right)|3\rangle$$

Perguntas importantes:

- No exemplo 1, qual a probabilidade de observar o estado $|0\rangle$ ao medir o sistema?
- No exemplo 2, qual a probabilidade de observar o estado $|k\rangle$? $(k = 0, 1, 2, 3)$