Fundamentos de Computação Quântica:

Linguagem, Conceitos e Aplicações

Guilherme T. Goedert
goedert@roma2.infn.it
gtgoedert.com

The Cyprus Institute
RESEARCH·TECHNOLOGY·INNOVATION

RWTH AACHEN UNIVERSITY

Università di Roma Tor Vergata

Seminário EMAP / FGV

20/06/2022

Objetivos

- Tecnologias Quânticas estão avançando rapidamente em Computação e Informação;
- Adoção será gradativa, mas profundamente impactante para ciência, computação, comunicações e cibersegurança;
    - Data Science e IA;
    - Cibersegurança;
    - Desenvolvimento de drogas e materiais;
    - Otimização;
    - Logística;

Ao fim deste seminário, você estará ciente:

- das vantagens, aplicações e limitações desta tecnologia;
- dos princípios fundamentais e linguagem matemática que baseiam QC;
- Princípios da Superposição e Entrelaçamento, suas consequências positivas e negativas para QC;

Estará equipado para aprofundar conhecimento em QC e fazer juízo sobre as tendências emergentes neste campo!

Sumário

Organizamos esta apresentação em torno de quatro perguntas principais

- O que são qubits e como são representados estados quânticos?
- Como os princípios da Teoria Quântica refletem nas vantagens e limitações da Computação Quântica?
- Quais são as tecnologias sendo desenvolvidas e o que esperar?
- Como computadores baseados em um fenômeno intrinsecamente aleatório produzem resultados consistentes, e como esses novos computadores são programados?

O que são qubits e como são representados estados quânticos?

Bit:

- Unidade fundamental de informação clássica
- Realizado por um sistema que pode ser configurado em dois estados:
  0/1, +/-, Open/Closed, True/False
- Derivado da Teoria Clássica da Informação criada por Claude Shannon

Qubit:

- Unidade fundamental de informação Quântica;
- Realizada por sistemas quânticos de duas fases/níveis:
  spin de elétrons/núcleos e outras moléculas,
  polarização de photons,
  carga/corrente/energia em supercondutores
- Ocorrem transições espontâneas de estado, de modo que o processo de medida de um estado é aleatória

Princípio da superposição:
O estado de um sistema quântico **isolado** existe como superposição (combinação linear) de todas as suas possíveis configurações.

Figure source:
https://culturacolectiva.com/history/schrodinger-cat-theory-explained/

Princípio da Superposição

Formalmente:

- Observáveis (e.g. posição, momento, energia etc.) são funcionais auto-adjuntos de espectro discreto;

$$|\psi\rangle = c_0|\lambda_0\rangle + c_1|\lambda_1\rangle$$

- Possíveis configurações do sistema são autovetores de um Observável, e seus autovalores correspondem aos seus respectivos valores quando medidos;
- Ao efetuar uma medição, o sistema colapsa para uma das configurações possíveis, e o autovalor correspondente é o valor medido;
- Probabilidade de obtermos um valor do observável (regra de Born):

$$p(\lambda_i) = |c_i|^2$$

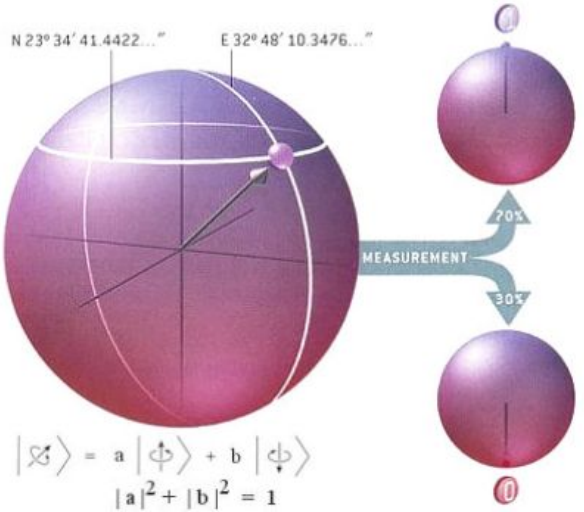
Representação de Estados Quânticos

Qubits:

- Podem ser implementados usando qualquer sistema quântico com dois autoestados:

$$|0\rangle, \quad |1\rangle$$

- Existem ao menos 15 diferentes implementações;
  - ❖ Supercondutores (carga, corrente, E)
  - ❖ Photons (polarização, estado Fock)
  - ❖ Sistemas de Spin (núcleos, elétrons)
  - ❖ Armadilhas de Íons



Esfera de Bloch

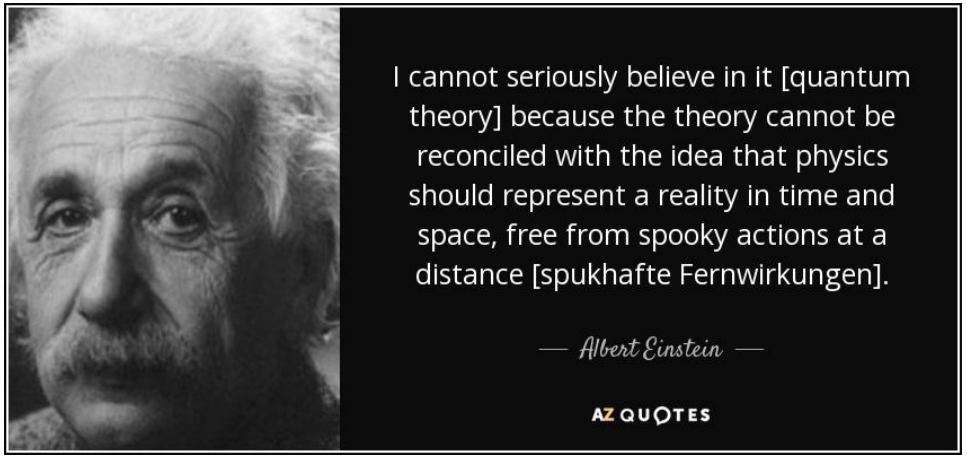
Figure Source: https://universe-review.ca/R13-06-qbit.htm

Representação de Qubits

Como os princípios da Teoria Quântica refletem nas vantagens e limitações da Computação Quântica?

Entrelaçamento Quântico

- Duas partículas entrelaçadas apresentam **correlação em suas observações, independente da distância em que se encontram;**
- Ao jogar cara ou coroa com duas moedas, o resultado de uma moeda é independente do resultado de sua companheira. Isso pode ser muito diferente em escala quântica: ao jogar uma “moeda quântica”, a medição colapsa informação de todo o sistema!
- **Essa interação é mais rápida que a velocidade de luz!**



- Dados sistemas quânticos A e B, o sistema composto AB será descrito pelo espaço de Hilbert $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$
- “Estados produto”: $\psi_A \otimes \psi_B$
- Existem estados no espaço composto que não podem ser definidos como estados produto (e.g. a própria identidade). Mas os produtos das bases dos espaços individuais formam base para o espaço composto.

$$|\psi\rangle = c_{0,0}|0,0\rangle + c_{0,1}|0,1\rangle + c_{1,0}|1,0\rangle + c_{1,1}|1,1\rangle$$

- Estados entrelaçados são aqueles que não podem ser fatorados como produtos de estados dos sistemas constituintes.

Sistemas Compostos e Entrelaçamento Quântico

- Para um sistema de três qubits:

$$|\psi\rangle = c_1|0,0,0\rangle + c_2|0,0,1\rangle + c_3|0,1,0\rangle + c_4|1,0,0\rangle + c_5|0,1,1\rangle + c_6|1,0,1\rangle + c_7|1,1,0\rangle + c_8|1,1,1\rangle$$

- Sistema composto de N qubits entrelaçados codifica informação em 2^N bases!

- Desafio: **Decoerência**!
  - Ao mensurar um dos estados constituintes, todo o sistema colapsa e perde informação!
  - Podemos verificar o estado do primeiro gato:

$$\frac{1}{2}\{|\text{🐱🐱}\rangle + |\text{🐱🐈}\rangle + |\text{🐈🐱}\rangle + |\text{🐈🐈}\rangle\}$$

  - Depois de observar apenas o primeiro gato, o sistema inteiro colapsa para

$$\frac{1}{\sqrt{2}}\{|\text{🐱🐱}\rangle + |\text{🐱🐈}\rangle\} \quad \text{Ou} \quad \frac{1}{\sqrt{2}}\{|\text{🐈🐱}\rangle + |\text{🐈🐈}\rangle\}$$

Aumento exponencial de dados e Decoerência

Decoerência e Fragilidade

- Interações com meio ambiente são efetivamente observações, colapsando estados!
  - Esta é a razão pela qual fenômenos quânticos são observados apenas em escala microscópica!

- Computadores quânticos precisam de rigoroso controle ambiental:
  - Sistemas a base de supercondutores funcionam apenas em temperaturas ~ mK
    Espaço sideral ~ 2.7 K (**−270.45 °C**)
  - Isolamento eletromagnético e contra choques avançado

- Mesmo com extenso controle ambiental, isolamento perfeito é impossível!
  - Caso contrário, manipulação e observação também seria impossível...
  - **O tempo de decoerência** varia muito com sistema, tipicamente ~10^{-3} a 10^{-9} seg.
  - Sistemas mais estáveis, no entanto, possuem frequências menores para execução de operações.

- **Decoerência causa perda de informação e erros!**

Vantagens

- **Estados Quânticos encapsulam volume exponencial de informação!**
  - Imenso custo computacional para simuladores quânticos;
  - Grande desafio para simuladores moleculares clássicos, mas possíveis para QC.
  - 71 qubits encapsulam mais informação do que somos capazes de armazenar com toda a memória RAM na Terra!

- Operações sobre um constituinte de um sistema entrelaçado afetam todo o sistema!
  - Economia e aceleração em operações;

- **Superdense Coding:**
  - Protocolo de Comunicação - comunica N bits ao transmitir número muito menor de qubits
  - Supõem que as duas partes compartilharam recursos entrelaçados, sendo que um será transmitido e o outro será usado pelo destinatário como controle para decodificação
  - **Comunicação segura!**
  - Quantidade de informação transmitida por sistema quântico não é exponencial (Teorema de Holevo)

Quais são as tecnologias sendo desenvolvidas e o que esperar?

Supercondutores

Microsoft

IBM

Google

D:Wave
The Quantum Computing Company™

Photons

XANADU

Armadilhas de Ions

Honeywell

IONQ

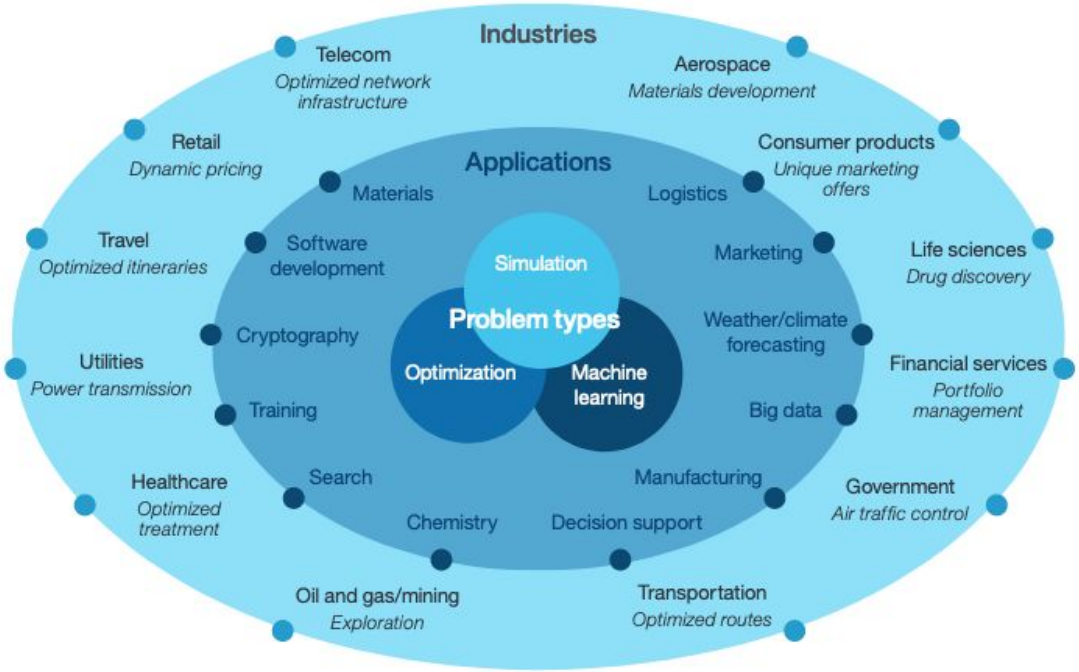


Figure source: https://www.ibm.com/thought-leadership/institute-business-value/report/quantumleap

Aplicações

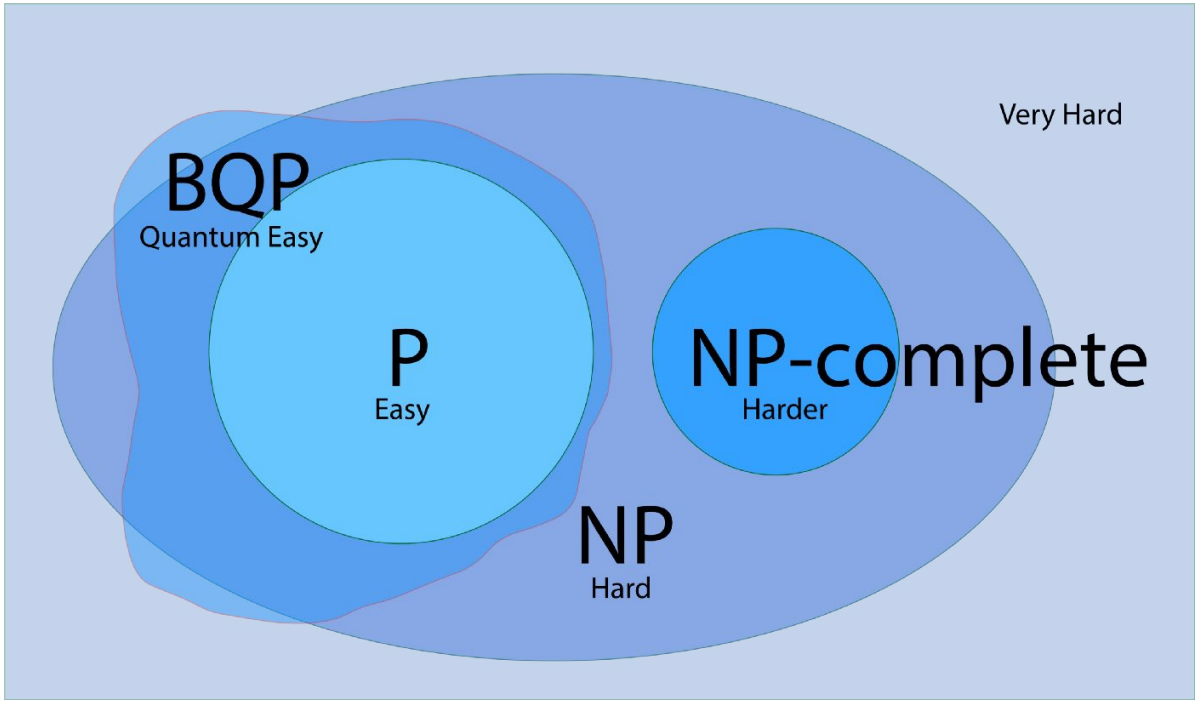
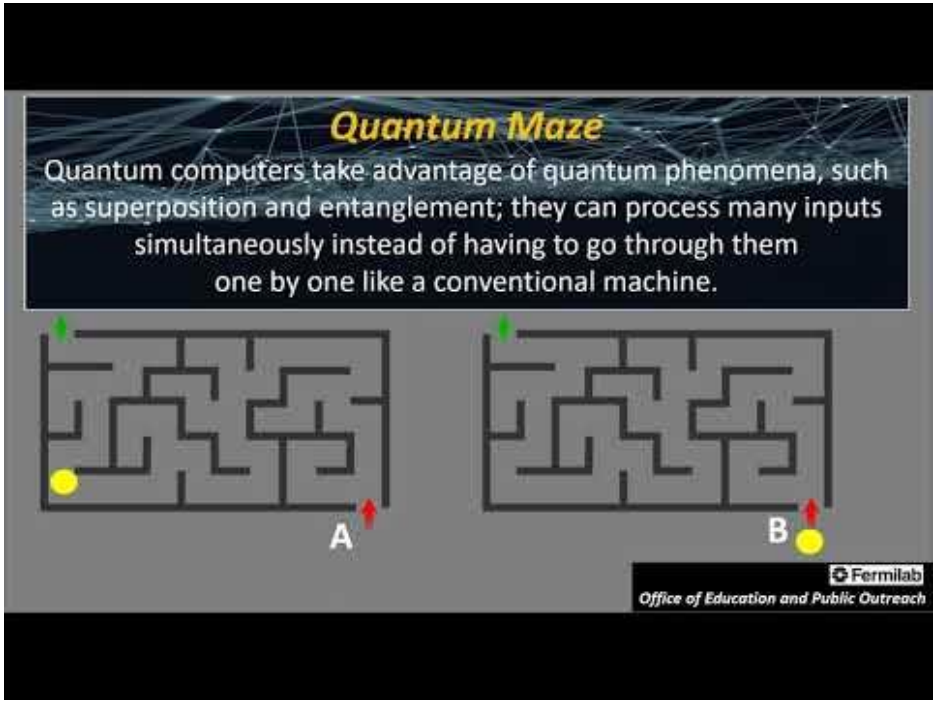


Figure source: https://www.ibm.com/thought-leadership/institute-business-value/report/quantumleap

- P: tempo de execução limitado por polinômio
- NP: tempo de execução polinomial em máquina não determinística
  - Busca exaustiva
  - Verificação é P
- BQP: tempo polinomial em CQ com erro limitado

Complexidade de Problemas



Busca por caminhos

Descubra o Segredo: 101001

- Solução “Humana”: busca exaustiva de 2^6 combinações…
- Computador Clássico: 6 iterações de AND

```
  101001
AND 000000
  000001
```

- **Computador Quântico precisa de apenas uma tentativa, não importa o tamanho do segredo! (Algoritmo de Bernstein-Vazirani)**

Supremacia Quântica é definida como uma instância em que um QC é capaz de solucionar um problema que seria impossível para um CC em tempo viável!
(Independente de sua utilidade…)

Exemplo: Fatoração de Inteiros (Algoritmo de Schor):

- CC ~ $2^{O(N^{1/3})}$
- QC ~ $O\big((\log N)^2(\log\log N)(\log\log\log N)\big)$

Schor já foi implementado! Estamos em risco de colapso criptográfico?!

- 2001 (IBM) fatorou 15 = 5 x 3 (computador de 7 qubits)
- 2001 dois outros grupos fatoraram 15 com qubits photonicos
- 2012 foi fatorado 21, record!!
- 2019 IBM fatora 35!!
  ….. Não…… Falhou por acúmulo de erros!

Schor depende de computadores tolerantes a erros!

- Estamos a décadas deste ponto:
  - Avanços na engenharia dos portões lógicos para diminuir taxa e erros;
  - Métodos de detecção e correção de erros em execução (grande aumento de qubits necessários);

- Avanços consideráveis estão sendo feitos em métodos de criptografia pós-quântica, estes novos métodos devem ser implementados muito antes de QC serem capazes de colocar segurança em risco;

- Comunicação Quântica também traz novas soluções seguras de comunicação:
  - Mensagens interceptadas colapsam!
  - Não se pode “copiar” um estado quântico (No Cloning Theorem);
  - Superdense coding.

Estamos seguros!

- **Primeiro em 2019 - Google**
  - 53 qubits
  - Amostragem de números aleatórios
  - Estimativa de 10.000 anos para o melhor CC
  - Bastante controverso

- **Mais recente em 2022 - Borealis (Xanadu)**
  - 216 qubits
  - Maior QC photônico já construído
  - Disponibilidade pública pela nuvem
  - Gaussian Boson Sampling
    - CC: 9.000 anos ($2{,}83 \times 10^{11}$ seg)
    - Xanadu: 36 microseg.
  - Xanadu foi 50 milhões de vezes mais rápido que demonstrações anteriores de QC photônicos, demonstrando grande avanço tecnológico.

Mais recente exemplo de supremacia quântica: Borealis da Xanadu

Como esses novos computadores são programados?

- Uma CPU executa suas instruções diretamente, as coisas são bem diferentes para QPUs…

- QPU (Quantum Processing Units)
  - Combinação de Eletrônicos de Controle e Memória Quântica (Qubits)
  - Integrado a um sistema Clássico que
    - converte circuitos para formas digeríveis a QPU,
    - coleta e processa resultados.

- A QPU recebe instruções sobre qual Circuito Quântico deve produzir e retorna medições ao fim de cada execução deste circuito.

- Quantum Gate:
  - Operação a ser executada sobre um ou mais qubits, modificando estados quânticos sem causar colapso de informação;
  - São representados por Operadores Unitários:
    - Preservam a norma dos estados e formulação probabilística;
    - Efetua uma rotação do estado na representação da Esfera de Bloch;
    - Possíveis estados medidos são os mesmos, muda-se apenas as probabilidades de serem observados.

- Quantum Circuit:
  - Conjunto de qubits, bits, Quantum Gates e medições sobre o sistema, organizados sequencialmente

- Quantum Program:
  - Conjunto de instruções (script clássico) que codifica criação de Circuitos, suas repetidas execuções (shots) e análise dos dados coletados.

- Evolução de sistemas quânticos é governada pela Equação de Schrödinger:

$$i\hbar\frac{d}{dt}\psi(t) = H\psi(t).$$

Para Hamiltoniano constante

$$|\psi\rangle = e^{-iHt/\hbar}|\psi_0\rangle$$

- Quantum Gate: Operadores Unitários $U = e^{-iHt/\hbar}$ que modificam estados de qubits

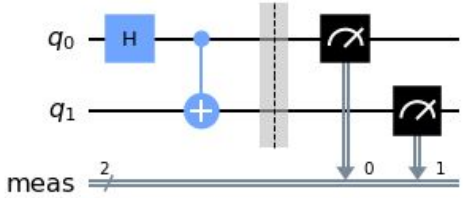
$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \qquad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H|0\rangle = |+\rangle \qquad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

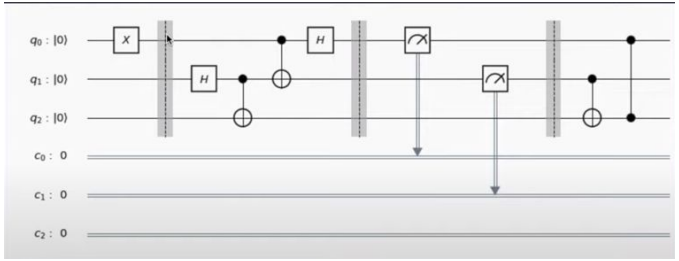
$$H|1\rangle = |-\rangle \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Exemplos de Quantum Gates

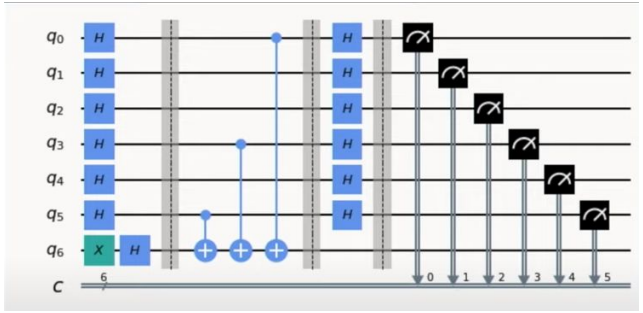
- Entrelaçamento de dois Qubits



- Teletransporte Quântico



- Bernstein-Vazirani

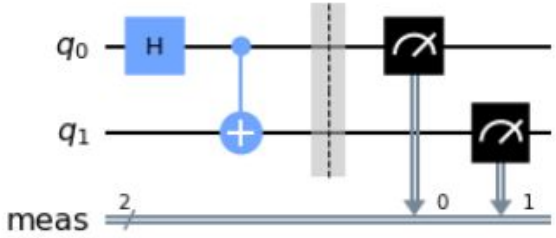


Exemplos de Circuitos Quânticos

```
from qiskit import IBMQ, QuantumCircuit, transpile
from qiskit.tools import job_monitor
from qiskit.visualization import plot_histogram, plot_gate_map
```

```
# Loading your IBM Quantum account(s)
IBMQ.load_account()
provider = IBMQ.get_provider(hub='ibm-q', group='open', project='main')
backend = provider.get_backend('ibmq_lima')
```

```
qc = QuantumCircuit(2)
qc.h(0)
qc.cx(0, 1)
qc.measure_all()
qc.draw(output='mpl')
```



Exemplo de Programa Quântico (Entrelaçamento)

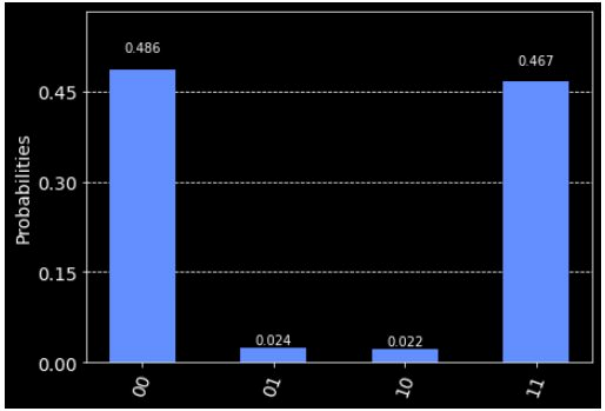
```
# run job on real hardware
job = backend.run(transpile(qc, backend=backend), shots=1024)
```

```
from qiskit.tools.monitor import job_monitor
job_monitor(job)
```

```
Job Status: job has successfully run
```

```
job = backend.retrieve_job('62af9f4ccb0a7b89a40a5c86')
```

```
import matplotlib.pyplot as plt
plt.style.use('dark_background')
plot_histogram(job.result().get_counts())
```



- Este programa cria entrelaçamento entre dois qubits e observa seus valores
- Idealmente, haveria correlação perfeita entre os valores medidos e observaríamos apenas 00 e 11
- Como o Hardware ainda apresenta erros e circuito não possui correção automática, ainda observamos alguns shots nos valores não desejados

Exemplo de Programa Quântico (Entrelaçamento)

Demonstrando Algorítmo de Bernstein-Vazirani

Demonstração!

Ainda não temos metodologia geral para desenvolvimento de Algoritmos Quânticos

Mas temos uma boa ideia:
Amplificação de Probabilidades!

Codificamos possíveis configurações em elementos de base do sistema, e executamos circuitos que amplificam a probabilidade de observarmos configurações de interesse

Essas operações são aplicadas sobre todas as configurações de forma eficiente graças a superposição, e podem se “comunicar” graças ao entrelaçamento. Circuitos inteligentes, amplificam a chance de encontrarmos a agulha no palheiro.

Exemplo: “e se não alimentarmos o gato de Schrödinger?”

Obrigado!

Contato: goedert@roma2.infn.it
gtgoedert.com

Leitura recomendada:

- Jack D. Hidary, “Quantum Computing: An Applied Approach”
- Michael Nielsen & Isaac Chuang, “Quantum Computation and Quantum Information”
- Maria Schuld & Francesco Petruccione, “Supervised Learning with Quantum Computers”
- “Decoherence Is a Problem for Quantum Computing, But ...”
- “When Quantum Computation Meets Data Science: Making Data Science Quantum”
- “How to Fix Quantum Computing Bugs”
- “The Real Reasons Quantum Entanglement Doesn't Allow Faster-Than-Light Communication”
- “Quality, Speed, and Scale: three key attributes to measure the performance of near-term quantum computers” arXiv:2110.14108