

# Fundamentos de sistemas de comunicações baseados em algoritmos quânticos

Daniel Coutinho - IC - Licenciatura em Física - Petrópolis

Eder Oliveira - TCC - Engenharia Eletrônica - Maracanã

Jose Antonio - Doutorando - PPGIO - Maracanã

Demerson Nunes - Professor - Departamento de Matemática - Petrópolis

Joao Dias - Professor - COTEL/DETEL/PPEEL - Maracanã

Centro Federal de Educação Tecnológica do Rio de Janeiro - Cefet/RJ

October 19, 2021

# Agenda

## Aula 1:

- Fundamentos dos sistemas de comunicações;
- Desafios dos sistemas 5G+ e 6G;

## Aula 2:

- Supremacia quântica;
- Origem da computação quântica
- Aplicações da computação quântica
- Principais algoritmos quânticos
- As regras do jogo

# Agenda

## Aula 3:

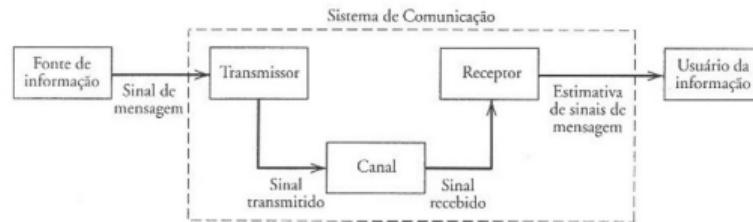
- Demonstração experimental de uso do computador quântico da IBM;
- Implementação experimental de circuitos de portas quânticas no computador quântico da IBM;

## Aula 4:

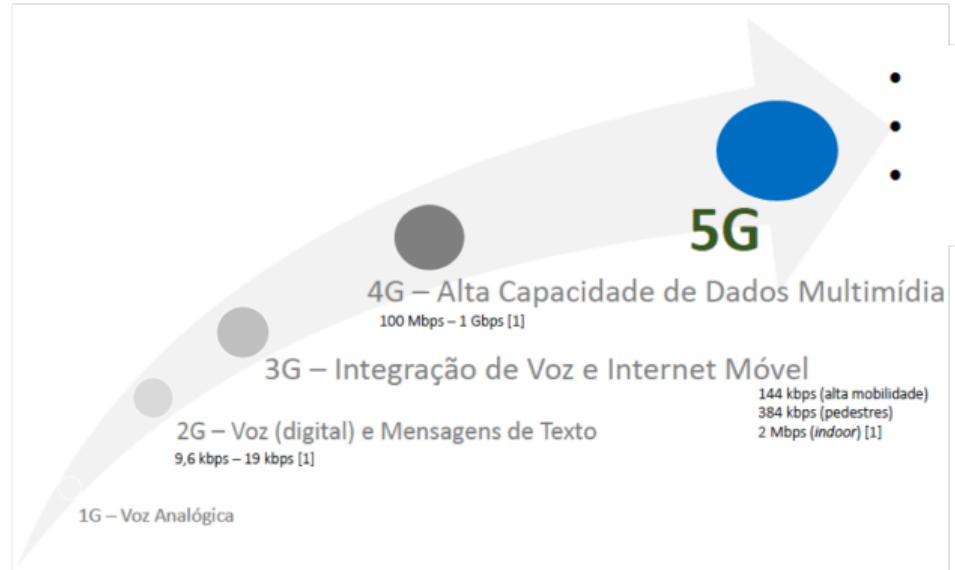
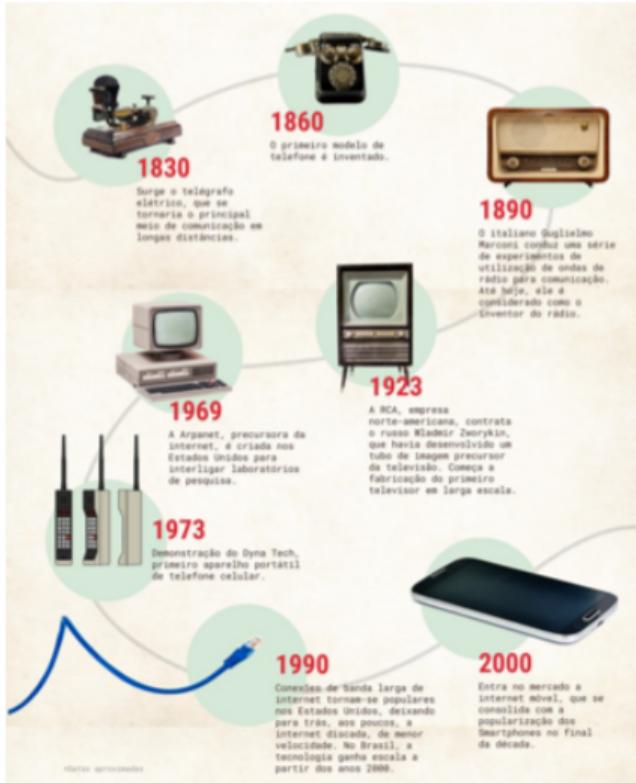
- Vantagens da computação quântica em relação a computação clássica;
- Aplicação de algoritmos quânticos em sistemas de comunicações;
- Comparação da complexidade computacional dos algoritmos;
- Análise de desempenho dos sistemas de comunicações baseados em algoritmos.

# Aula 1: Fundamentos dos sistemas de comunicações

- **fónte de información:** gera a mensagem que será transmitida;
- **Transmissor:** transforma a mensagem em um sinal robusto ao meio de transmissão;
- **Canal:** é o meio por onde o sinal será enviado;
- **Receptor:** recupera a mensagem no sinal recebido;
- **Usuário da informação:** é o destinatário da mensagem.



# A evolução dos sistemas de telecomunicações



# Evolução das arquiteturas de redes celulares

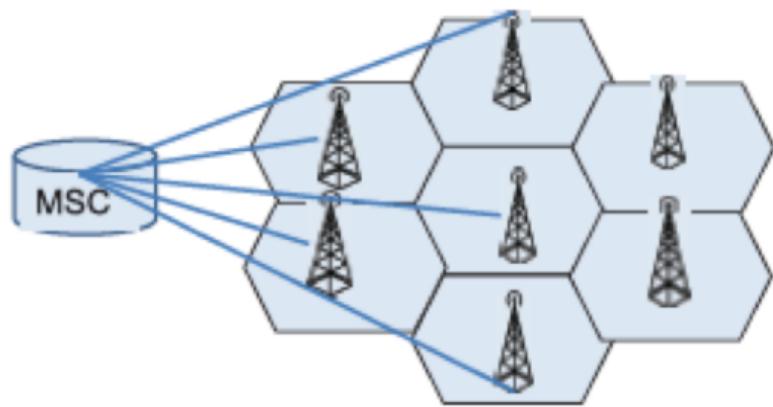


Figure: Rede wireless centrada na BS

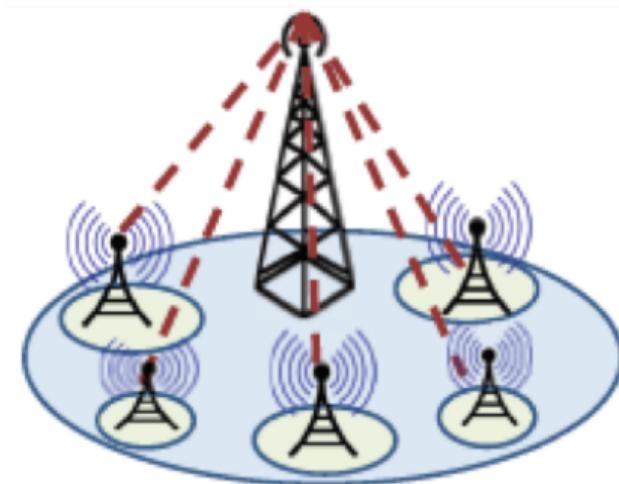
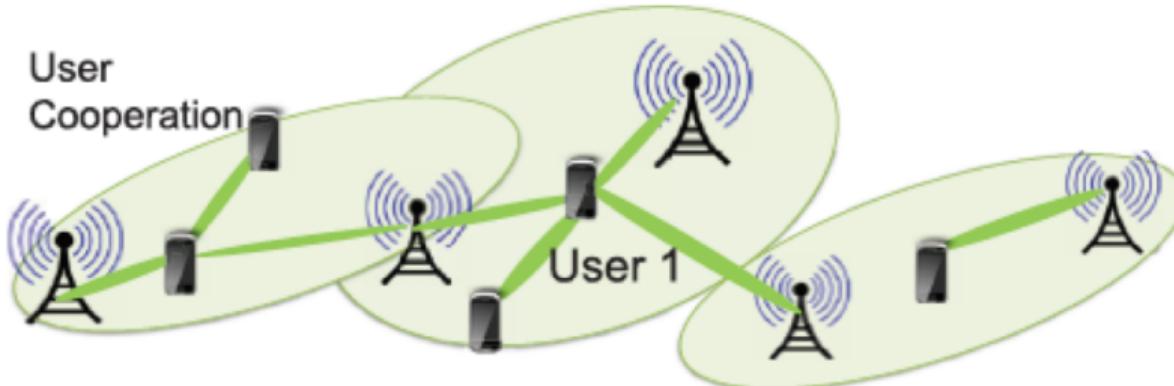


Figure: Rede de pequenas células

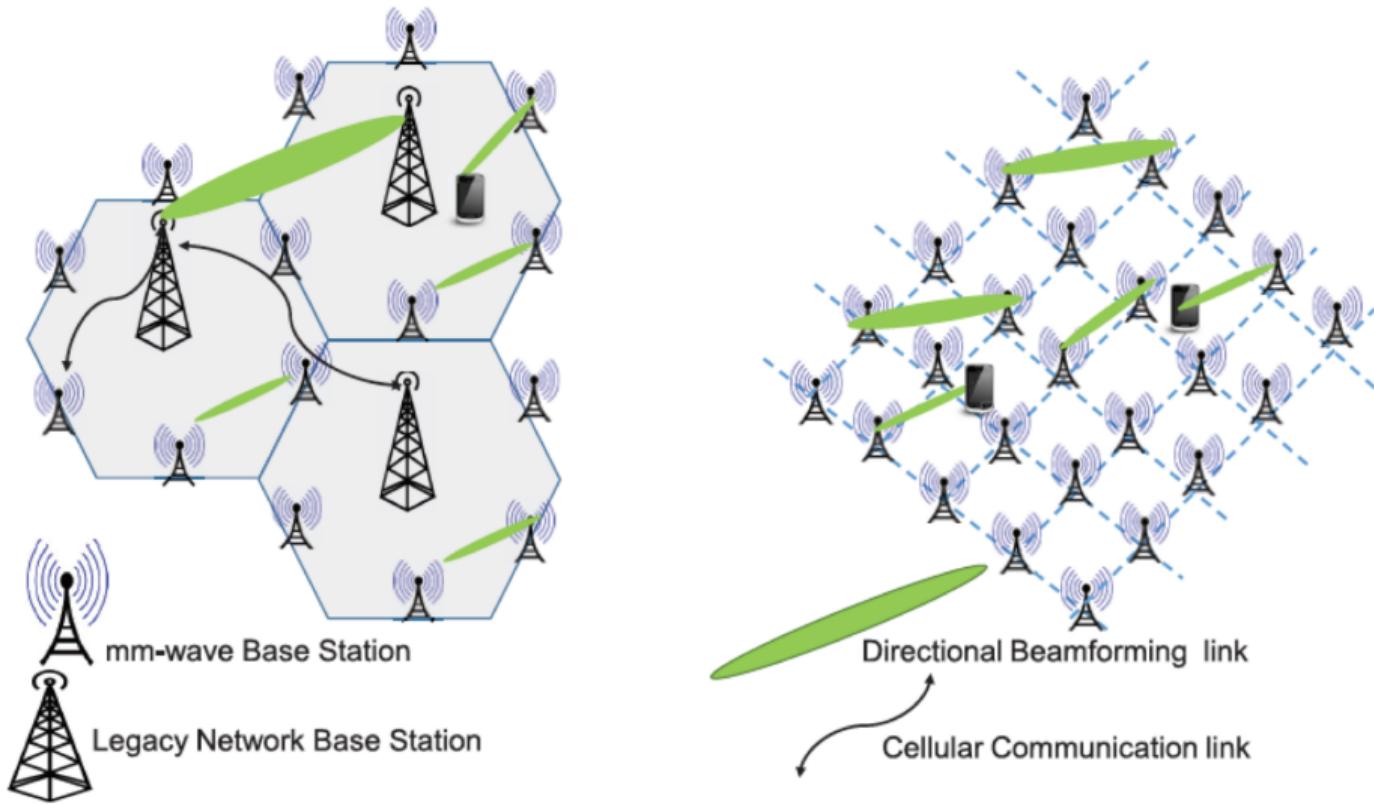
# Evolução das arquiteturas de redes celulares



User 1: Served Cooperatively by user centric & overlapping subset of BS

Figure: Rede wireless centrada no usuário

# Evolução das arquiteturas de redes celulares



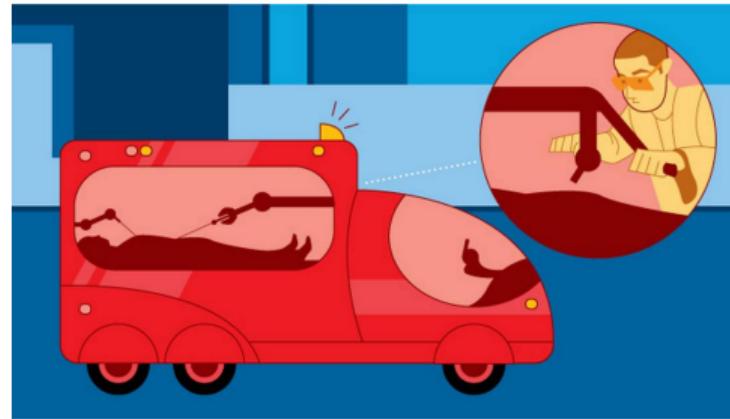
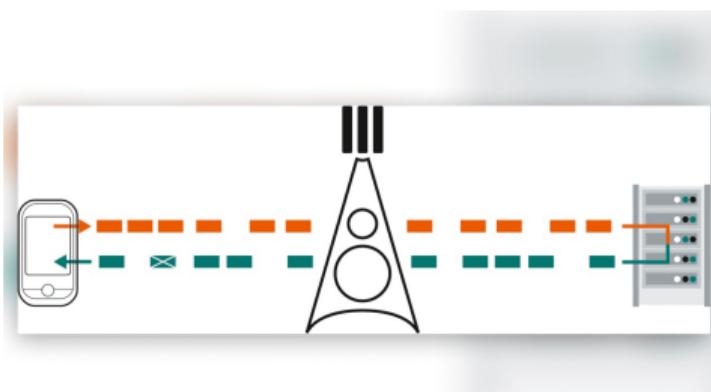
# Serviços alvo na tecnologia 5G

- **Banda Larga Móvel Aprimorada (eMBB):** As redes 5G têm como objetivo fornecer um aumento de 1000 vezes na taxa de transferência agregada e um aumento de 10 vezes na taxa de transferência de link individual em relação às redes sem fio de 4<sup>a</sup> Geração (4G).



# Serviços alvo na tecnologia 5G

- **Comunicações em baixa latencia ultra confiável (URLLC):** O fornecimento de URLLC é um novo paradigma de serviço oferecido em redes 5G. Tanto o aspecto de confiabilidade, com taxas de erro de pacote de  $10^{-5}$ , e latências de ponta a ponta de 1 ms visam oferecer suporte a novos casos de uso, como automação de fábrica, direção autônoma, *e-health*, automação predial e cidades inteligentes, para citar alguns.



# Serviços alvo na tecnologia 5G

- **Comunicação massiva entre máquinas (mMTC):** Com o advento da IoT, um grande número de dispositivos de baixa potência e baixa taxa de dados requerem uma conexão com a Internet. Esses dispositivos podem ser normalmente usados para aplicações de detecção de ambiente e medição de serviços públicos e requerem apenas comunicações intermitentes com pequenas cargas de dados.

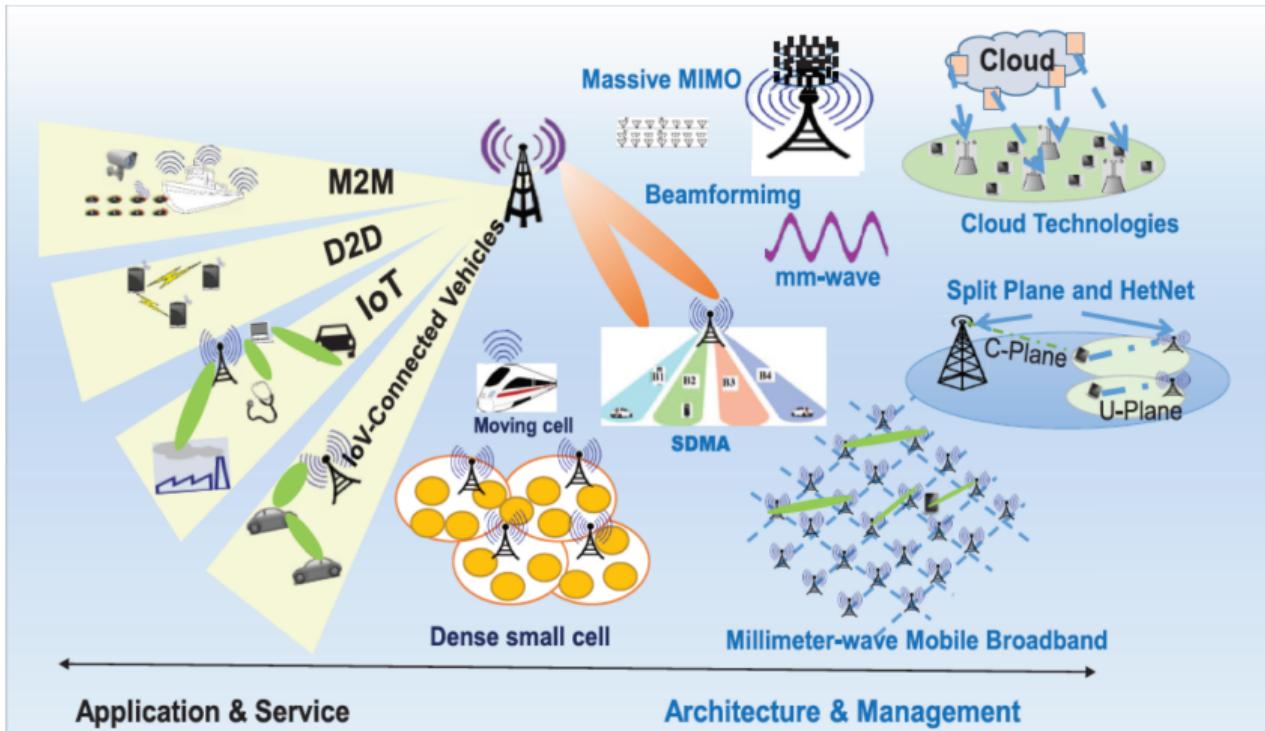


# Serviços alvo na tecnologia 5G

- **Internet tátil (TI)**: A IoT permite a interconexão de dispositivos inteligentes e a TI pode ser vista como uma evolução da IoT para permitir o controle em tempo real da IoT.



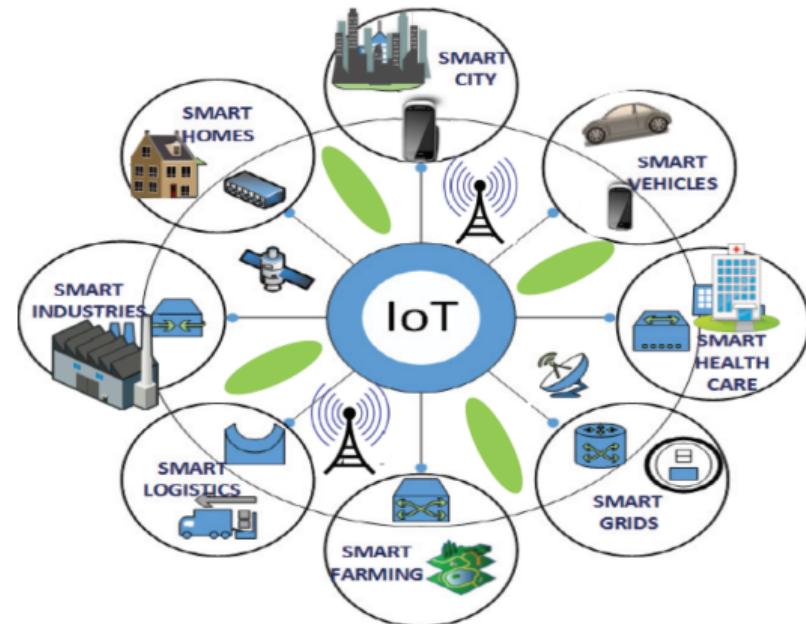
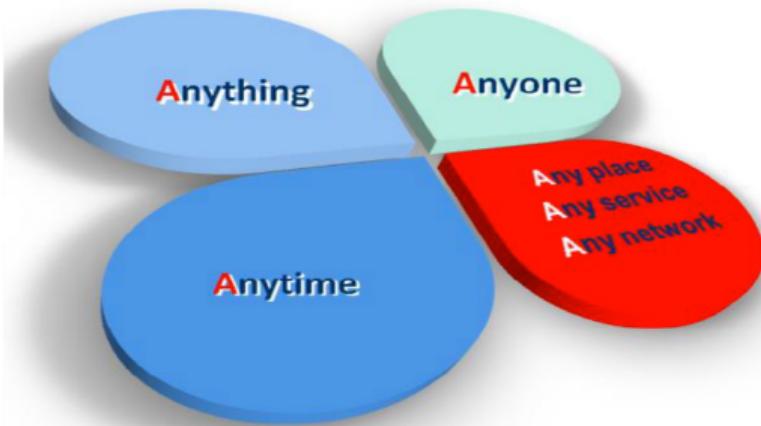
# 5G: Serviços e arquitetura



# Internet das coisas

IoT (Internet of Things) e IoE (Internet of Everything)

Connecting:



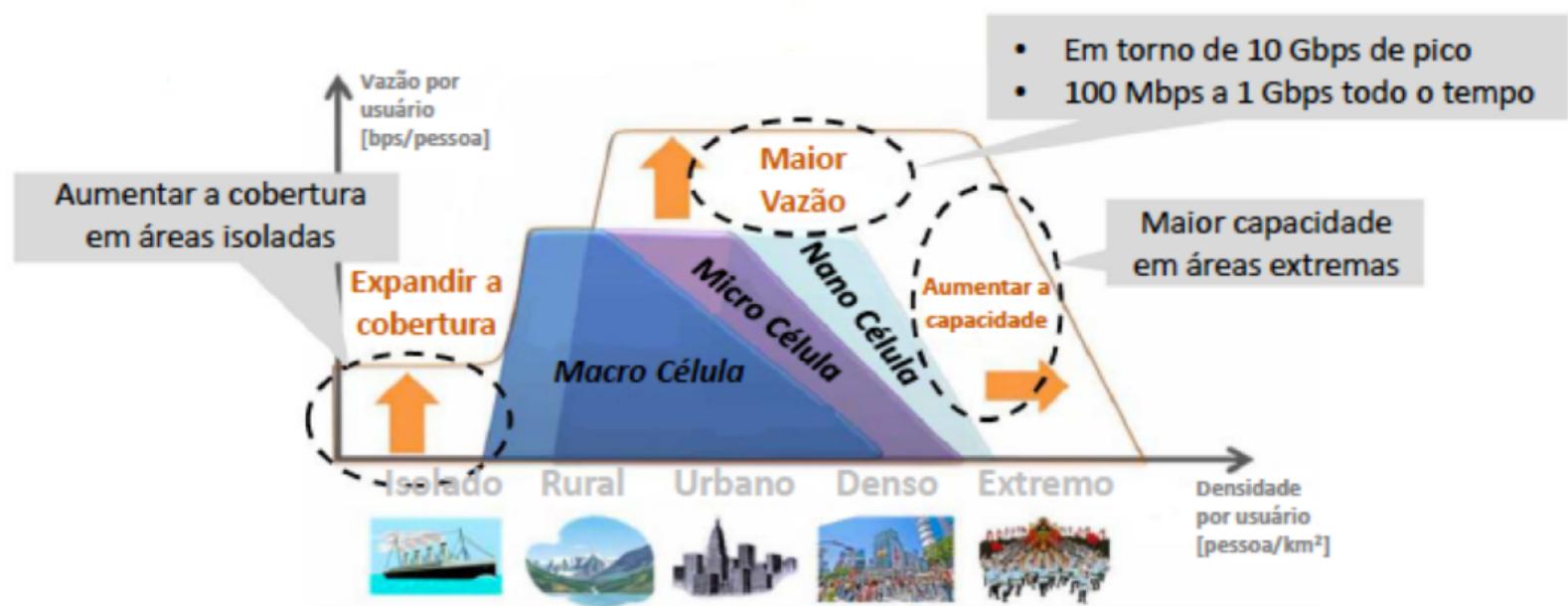
# Depois do 5G: Desafios abertos

- A comunidade científica já começou a discutir as metas para as redes de comunicações sucessoras do 5G: B5G, 5G+ e 6G. Os principais desafios observados são:
- **Taxa de transferência:** seguindo as tendências de evolução das gerações anteriores de redes móveis, espera-se que as metas de taxa de bits/s em redes 6G aumentem em uma ordem de magnitude em relação às de 5G. Além disso, os aplicativos de realidade virtual, uma vez amadurecidos, exigirão taxas de dados muito mais altas do que as prometidas pelo 5G. Por essas razões, taxas de dados de usuários individuais de até 100 Gbits/s são previstas para 6G.

# Depois do 5G: Desafios abertos

- **Capacidade de rede:** Tradicionalmente, a estratégia de densificação de células tem sido o principal habilitador para aumentar a capacidade de rede. No entanto, a redução do tamanho da célula (por exemplo, células minúsculas) também requer gerenciamento adequado da interferência intercelular aumentada para os usuários de extremidade da célula. Com o surgimento de cidades inteligentes, mMTC e usuários móveis em terra e no ar, a densificação de células por meio de BSs estáticos por si só não pode atender ao crescimento exponencial nas demandas de capacidade. Esse problema pode ser atenuado por redes celulares híbridas que empregam veículos aéreos não tripulados (UAVs) como BSs móveis.

# Depois do 5G: Desafios abertos

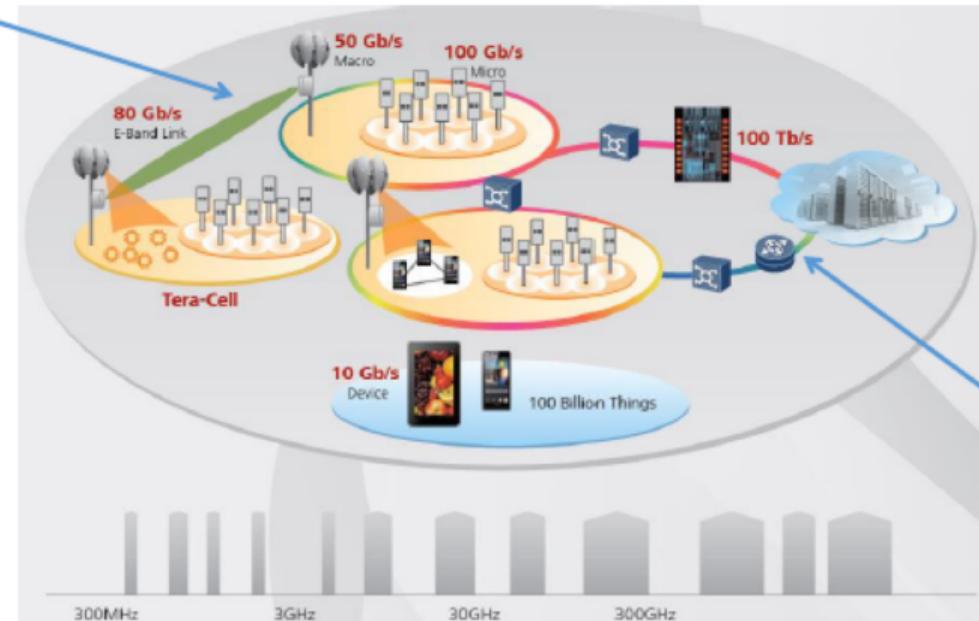


# Depois do 5G: Desafios abertos

- **Eficiência energética:** aumentar a eficiência energética da rede móvel ajuda a reduzir seus gastos operacionais e suas emissões de carbono. Para este fim, os esforços de projeto para redes 5G consideraram abordagens de eficiência energética para implantação de rede e alocação de recursos, incluindo novas tecnologias, como M-MIMO e redes heterogêneas ultradensas.
- **Backhaul e congestionamento de rede de acesso:** O tráfego de backhaul 6G exigirá redes de acesso equivalente a fibra óptica de latência muito baixa para suportar as altas taxas de dados e requisitos de qualidade de serviço nas comunicações fronthaul 6G.

# Depois do 5G: Desafios abertos

*Backhaul  
Sem Fio*



*Backhaul  
Fibra  
Óptica*

# Depois do 5G: Desafios abertos

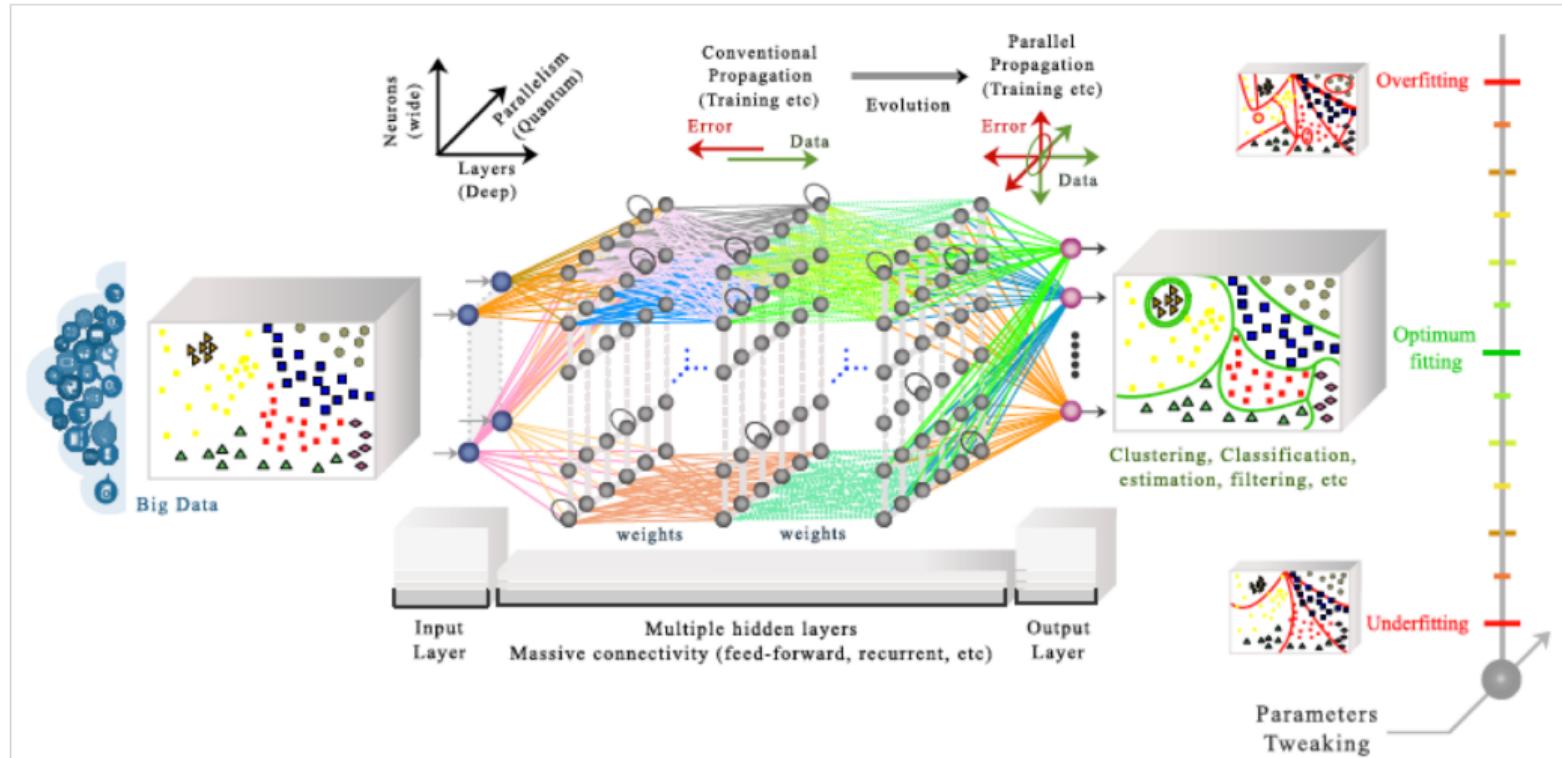
- **Segurança de dados:** uma enorme quantidade de dados do usuário é propagada e armazenada em redes móveis na forma de mensagens de voz e texto com geomarcação, bem como registros de atividades de aplicativos móveis. Proteger esses dados de bisbilhoteiros e seu uso não autenticado são de primordial importância. A fim de proteger os links de comunicação 6G, os esquemas de segurança da camada física podem ser implantados em conjunto com os esquemas de criptografia convencionais. Além disso, os esquemas baseados em *ML* para segurança cibernética e criptografia quântica são abordagens promissoras a serem exploradas para proteger os links de comunicação em futuras redes 6G.



# Depois do 5G: Tecnologias emergentes

- Trazer inteligência para a camada física dos sistemas de comunicação pode capacitar a estimativa inteligente de parâmetros, mitigação de interferência e gerenciamento de recursos.
- Uso de Aprendizado de Máquina (*Machine Learning - ML*) para a otimização das métricas de desempenho apresentadas como desafios abertos (taxa de dados, latência e confiabilidade) nos contextos de rádio cognitivo, redes heterogêneas, Internet da coisa (IoT) e comunicações máquina-à-máquina (M2M).
- Aprendizado de máquina (ML) é um braço da Inteligência Artificial (IA) na qual as máquinas aprendem, executam e melhoram suas operações explorando o conhecimento operacional e a experiência adquirida na forma de dados.

# Depois do 5G: Tecnologias emergentes



**FIGURE 3:** An example of deep, wide, and complex artificial neural network structure. Evolution from sequential to parallel data processing and optimum

# Depois do 5G: Tecnologias emergentes

- Na busca para atender às demandas cada vez maiores de comunicações rápidas, confiáveis, seguras, inteligentes e *verdes*; a demanda por alta capacidade computacional dos sistemas também aumentou rapidamente.
- O paralelismo inerente oferecido pelos conceitos fundamentais da mecânica quântica e as perspectivas demonstradas por meio de resultados recentes da computação quântica indicam claramente um potencial definitivo para superar os sistemas de computação convencionais.

# Depois do 5G: Tecnologias emergentes

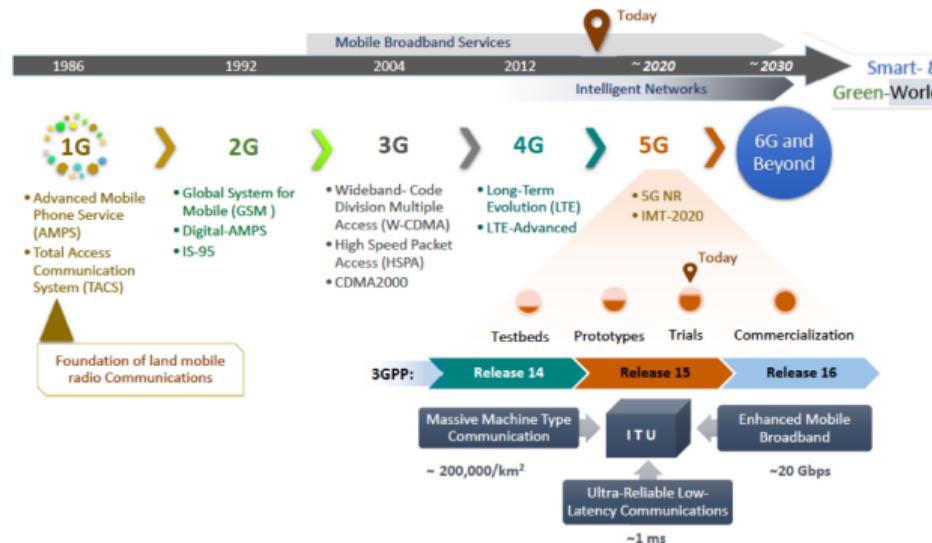
- Este imenso poder da computação quântica vem dos conceitos fundamentais de superposição quântica, entrelaçamento quântico e teorema da não-clonagem.
- O processamento paralelo de dados multidimensionais de grande porte pode ser convenientemente realizado por meio da computação quântica através de produtos tensoriais em espaços de grandes dimensões.
- As comunicações assistidas por algoritmos quânticos são projetadas para manter a promessa de atingir taxas de dados extremamente altas e segurança nos links de comunicações.

# Depois do 5G: Tecnologias emergentes

- A comunicação quântica é um ramo emergente da engenharia de telecomunicações, que foi motivada a partir dos princípios da mecânica quântica e é baseada na troca de estados quânticos.
- As comunicações assistidas por algoritmos quânticos podem aprimorar vários aspectos das redes de comunicação clássicas existentes, incluindo estimativa de canal, detecção multiusuário (MUD) ideal, o projeto de matriz de pré-codificação ideal e o roteamento ideal.

# 6G: Perspectivas e arquitetura

Essas redes não são apenas uma evolução das redes existentes, mas também introduzem novas tecnologias de comunicação revolucionárias destinadas a fornecer uma experiência imersiva ao usuário.



# 6G: Perspectivas e arquitetura

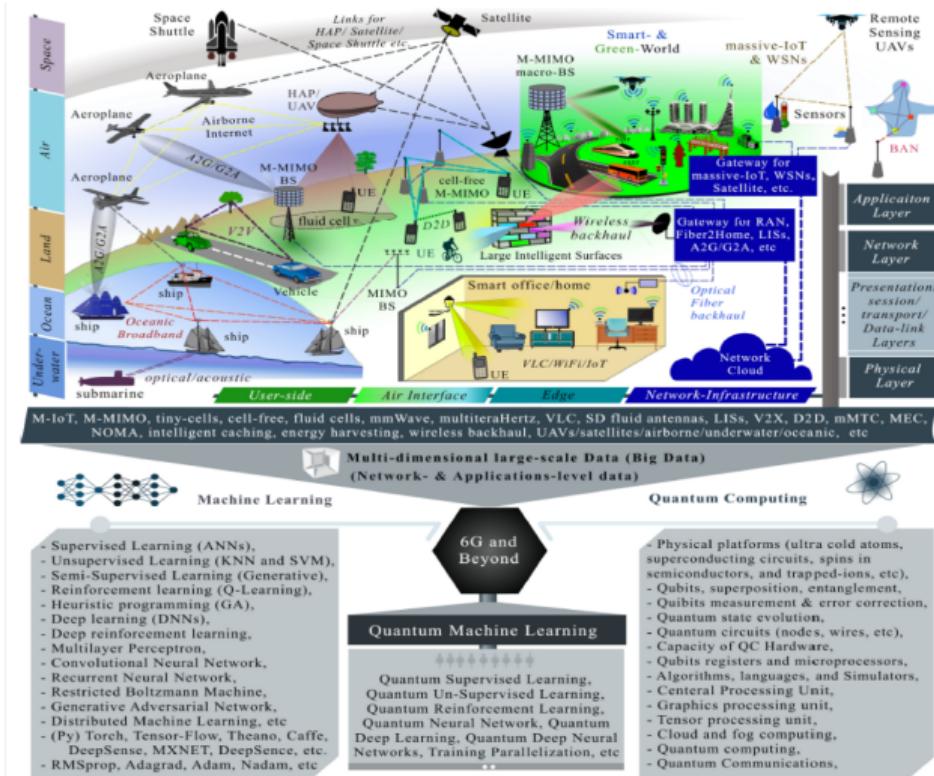


FIGURE 4: Illustration of different types, layers, sides, and levels of 6G communication networks indicating the applications and scope of QML.

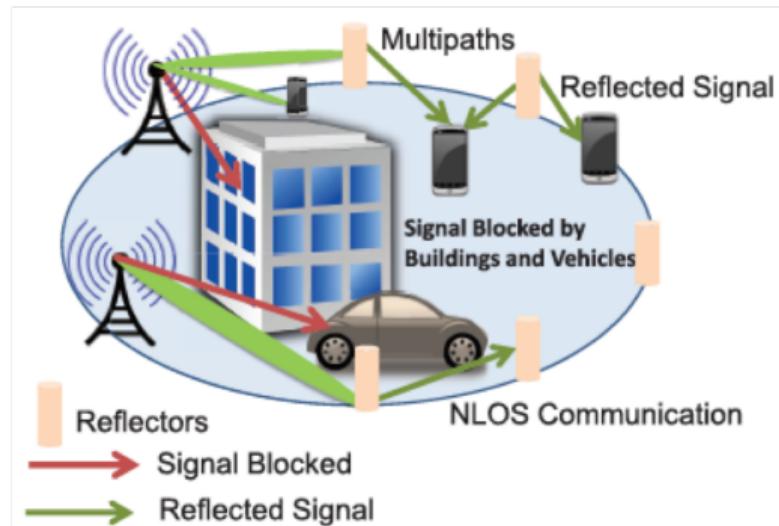
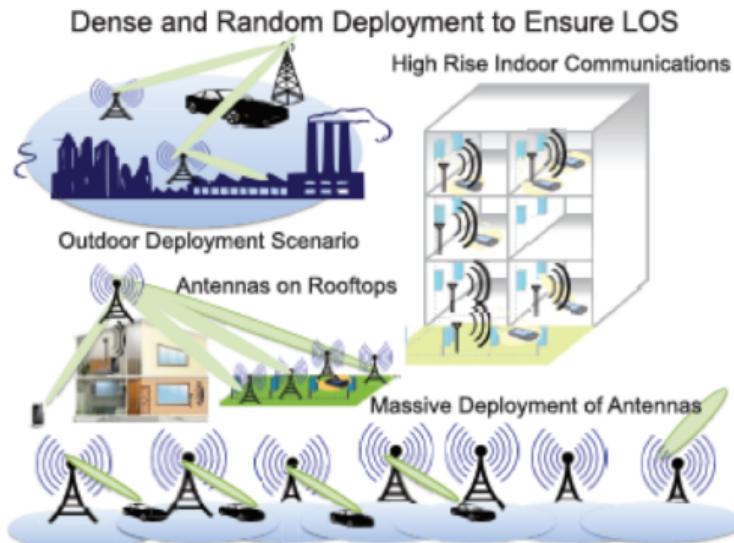
# Comunicações assistidas por algoritmos Quânticos

- A fim de tornar o aprendizado de máquina quântico (QML) uma realidade para as comunicações sem fio, o trabalho de pesquisa pode ser realizado por meio de simuladores de sistemas clássicos de comunicações com o fornecimento de recursos de computação quântica por dispositivos quânticos comercialmente disponíveis para a comunidade científica. Isso facilita o desenvolvimento de novos algoritmos QML em paralelo ao desenvolvimento de computadores quânticos.

# Estrutura proposta para redes 6G e linha de pesquisa

- **Infraestrutura de rede:** Sugere-se uma evolução das redes convencionais de sistemas móvel celular terrestre para as redes de comunicação móveis multi-espacó sem células, orientadas para serviços de rádio-óptica.
- **Cache proativo inteligente e computação móvel de borda:** o cache proativo inteligente se refere ao conceito de armazenamento dos dados em buffer nos nós (dispositivos IoT, BSs, etc.) de forma inteligente com base em sua popularidade/taxa de demanda.
- **Otimização Multi-Objetivo e Otimização de Roteamento:** Várias tarefas de análises de dados e ajustes de parâmetros envolvem otimização de funções objetivos com restrições.

# Estrutura proposta para redes 6G e linha de pesquisa



# Estrutura proposta para redes 6G e linha de pesquisa

- **IoT massivo e análise de grande volume de dados:** O conceito de futuras cidades inteligentes, inteligentes e *verdes* visa oferecer diversos novos serviços centrados nas pessoas para melhorar a qualidade de vida das pessoas.
- **Segurança e privacidade:** fornecer privacidade e segurança é um grande desafio no mundo emergente de tudo que está conectado à rede (por exemplo, a privacidade de big data em M-IoT).
- **Harmonização e interoperabilidade de redes:** As redes sem fio 6G são projetadas para serem conduzidas por auto-reconfiguração e interoperabilidade sob demanda com completa harmonização na coexistência de todos os seus predecessores.

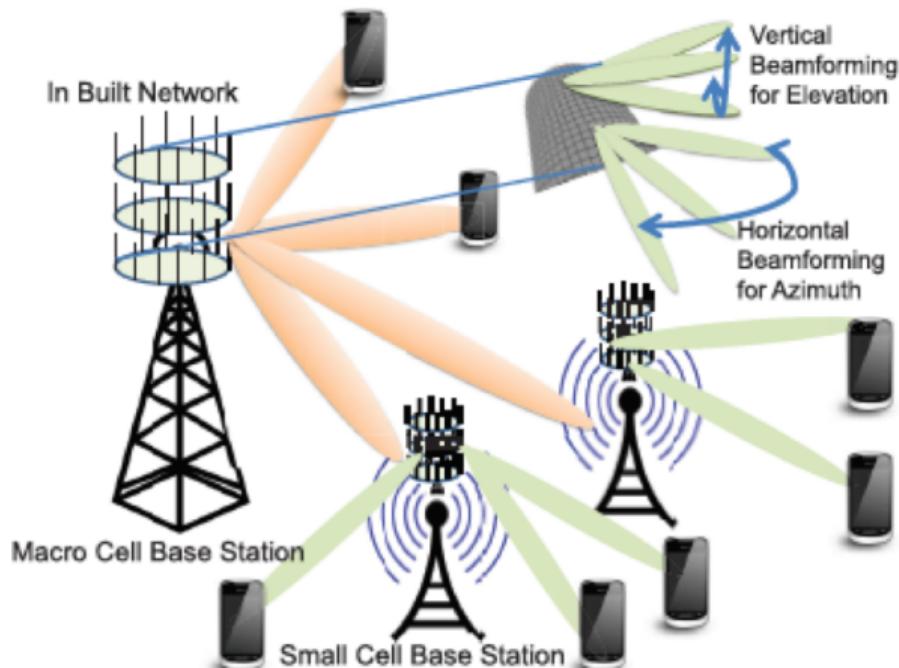
# Estrutura proposta para redes 6G e linha de pesquisa



# Estrutura proposta para redes 6G e linha de pesquisa

- **Paradigmas emergentes de metamateriais definidos por software:** com base em antenas configuráveis e Grandes Superfícies Inteligentes (LISs) combinados com sistemas de larga escala com múltiplas antenas operando em uma faixa muito ampla de espectro de frequência (microOnda, multiTerraHz, luz visível, etc) em sistemas distribuídos e não distribuídos redefinirão completamente a estrutura física da interface aérea.
- **Sistemas configuráveis de múltiplas antenas:** Os sistemas de larga escala com múltiplas antenas têm grande potencial para aumentar a capacidade e a eficiência energética.

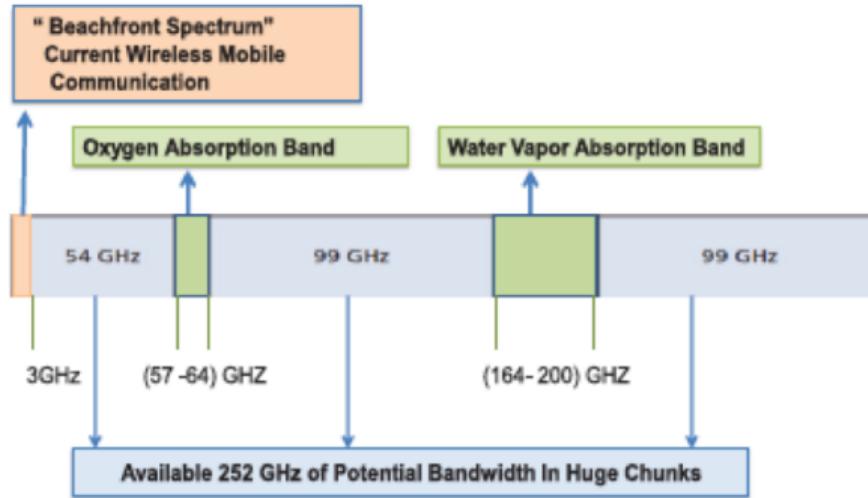
# Estrutura proposta para redes 6G e linha de pesquisa



# Estrutura proposta para redes 6G e linha de pesquisa

- **Comunicações ópticas, ondas milimétrica e TeraHz:** A abundância de espectro de rádio não utilizado disponível nas bandas de ondas milimétricas e TeraHz (THz) pode ser potencialmente utilizada para atender às crescentes demandas de capacidade.
- **Células minúsculas e comunicações livres de células:** As redes de comunicação sem fio são convencionalmente divididas em células para reutilização espacial eficiente de recursos de rádio (por exemplo, macro-, micro-, pico-, femto-, small-, tinycells, etc). O enorme aumento no número de dispositivos de rede e recursos limitados de rádio levaram a evolução das redes celulares para células de tamanho minúsculo (aproximando os usuários dos BSs) para um uso mais rigoroso dos recursos.

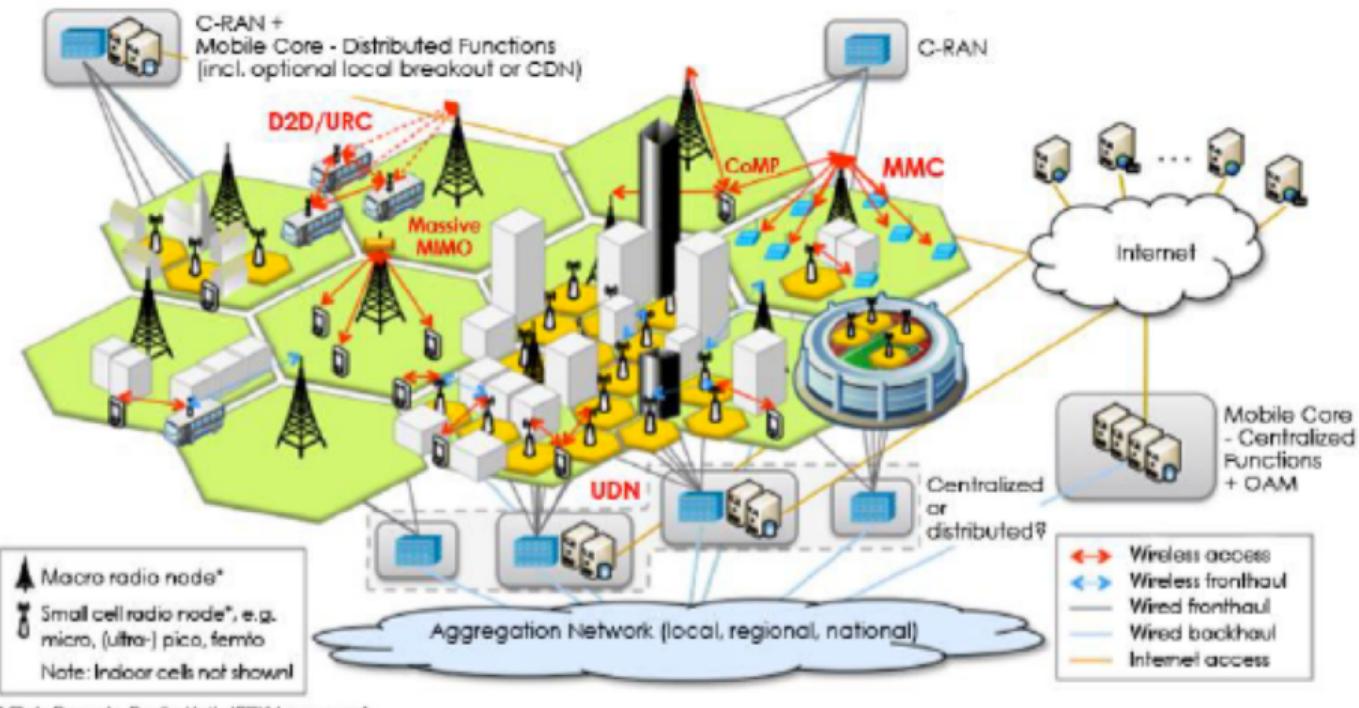
# Estrutura proposta para redes 6G e linha de pesquisa



# Estrutura proposta para redes 6G e linha de pesquisa

- **Auto-Codificação:** O aprendizado ponta a ponta visa representar todo o sistema de comunicação de um transmissor ao receptor com um único bloco de aprendizado. Este conceito fascinante permite o aprendizado do comportamento do transmissor e do receptor para otimizar em conjunto todas as operações com base em erro de ponta a ponta na precisão da recuperação.
- **Aprendizagem no lado do usuário:** Considerando a falta de recursos computacionais e de energia disponíveis nos nós de usuário, várias tarefas que são naturalmente do lado do usuário são hoje preferencialmente realizadas na estação de serviço ou no lado da nuvem da rede.

# Estrutura proposta para redes 6G e linha de pesquisa

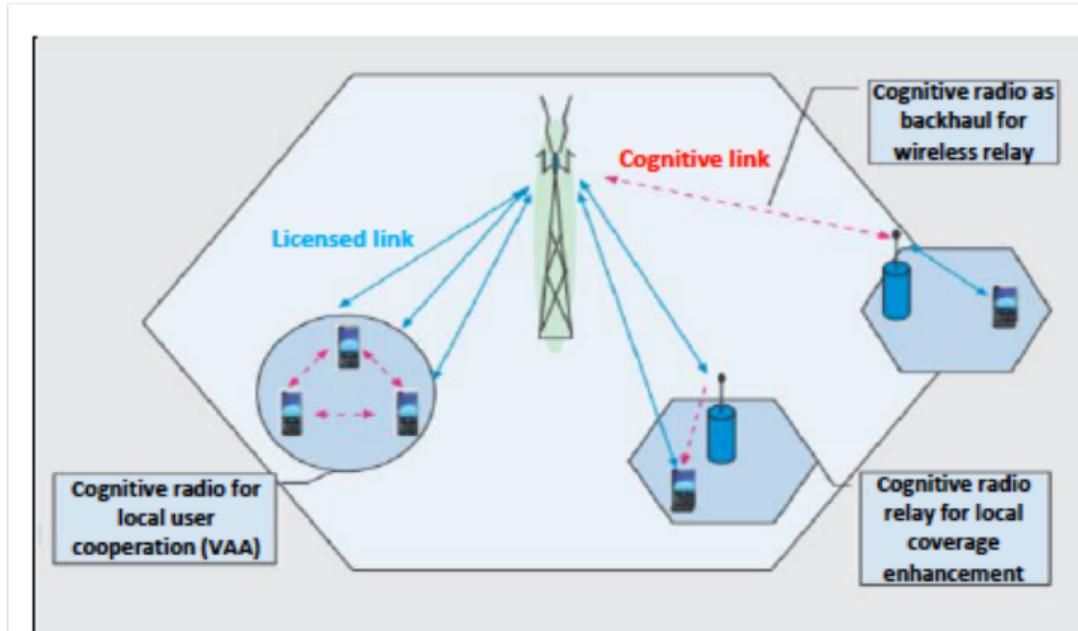


<https://www.metis2020.com/>

# Estrutura proposta para redes 6G e linha de pesquisa

- **Múltiplo acesso:** A necessidade de privilegiar o acesso do meio sem fio a uma quantidade massiva de usuários de forma ultraeficiente levou à evolução dos mecanismos de múltiplo acesso.
- **Rádio cognitivo inteligente e redes sem fio autossustentáveis:** o aproveitamento da inteligência para automatizar totalmente as redes de comunicação e permitir operações como autogerenciamento, autotimização, autoreparo e autoproteção, é uma necessidade clara para redes futuras. Os rádios cognitivos definidos por software são projetados para alcançar comunicação confiável com uso mínimo de recursos naturais por meio de operações inteligentes (por exemplo, reutilização espacial inteligente, etc.) aprendidas com o ambiente (por exemplo, análise de cena de rádio)

# Estrutura proposta para redes 6G e linha de pesquisa



Arquitetura e cenários de utilização de uma rede celular cognitiva.  
Exemplo de arquitetura cooperativa [7].

## Aula 2: Supremacia Quântica

**J. Preskill (Caltech):** Supremacia quântica consiste em demonstrar que um dispositivo quântico programável pode resolver um problema que nenhum computador clássico pode resolver em tempo viável;

# Computadores Quânticos



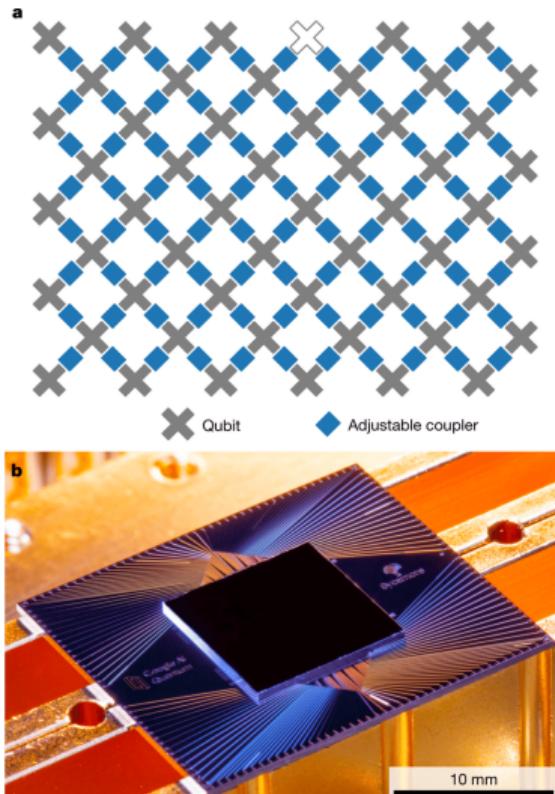
Figure: CQ Google - 53 qubits (2019)



Figure: "CQ" Jiuzhang - 76 qubits (2020)

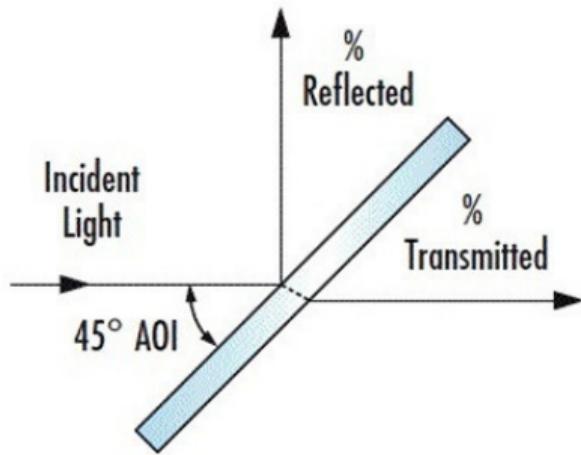
# Sycamore - Processador do CQ do Google (2019)

- Sycamore, foi capaz de executar em 200 segundos uma operação para calcular números aleatórios que o computador clássico mais poderoso da atualidade levaria 10 mil anos.
- [1] F. Arute,..., John M. Martinis. Quantum supremacy using a programmable superconducting processor. Nature, vol. 574, 2019.



# Jiuzhang - Computador Quântico Chinês (2020)

- Problema da amostragem de bosons (proposto por Aaronson et al - 2010).
- Implementação não programável de um circuito óptico com 76 fotons, 300 beam splitters, 75 espelhos.



# Jiuzhang - Computador Quântico Chinês (2020)

- A amostragem de bósons substitui as bolinhas por fótons, e os pinos por espelhos e prismas.
- Os fótons são disparados através da matriz e pousam em um “slot” no final, onde detectores registram sua presença.
- Devido às propriedades quânticas, um dispositivo com apenas 50 fótons poderia produzir tantas distribuições que computadores clássicos levariam bilhões de anos para prevê-las.

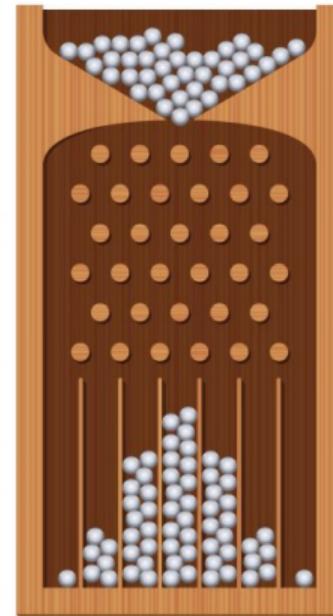
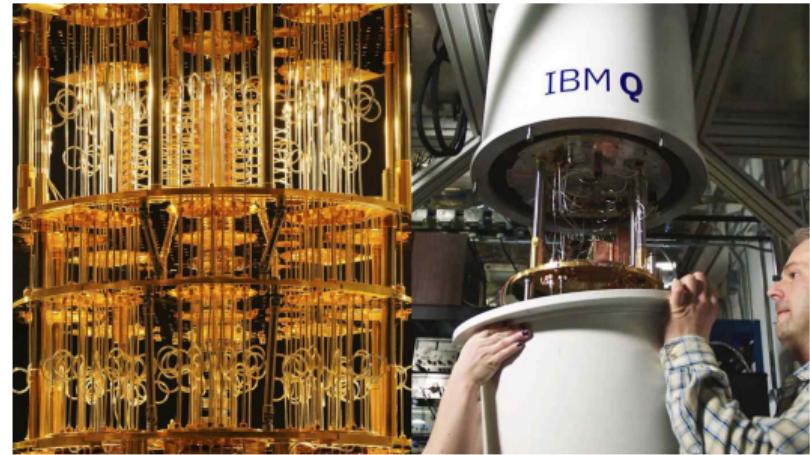


Figure: "Experimento de Galton"

# Computador Quântica da IBM - NISQ

- IBM Q Tokyo (20 qubits)
- IBM Q Melborne (14 qubits)
- IBM Q Tenerife (5 qubits)
- IBM Q Yorktown (5 qubits)



# IBM Quantum Experience - Composer

IBM Quantum Composer

File Edit Inspect View Share Setup and run

Untitled circuit Saved

Visualizations seed 5008

OpenQASM 2.0

Open in Quantum Lab

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[3];
creg c[3];
reset q[0];
reset q[1];
reset q[2];
h q[0];
h q[1];
cx q[0],q[1];
swap q[1],q[2];
s q[0];
```

Composer files

1 files New file +

Name Updated

Untitled circuit 2 minutes ago

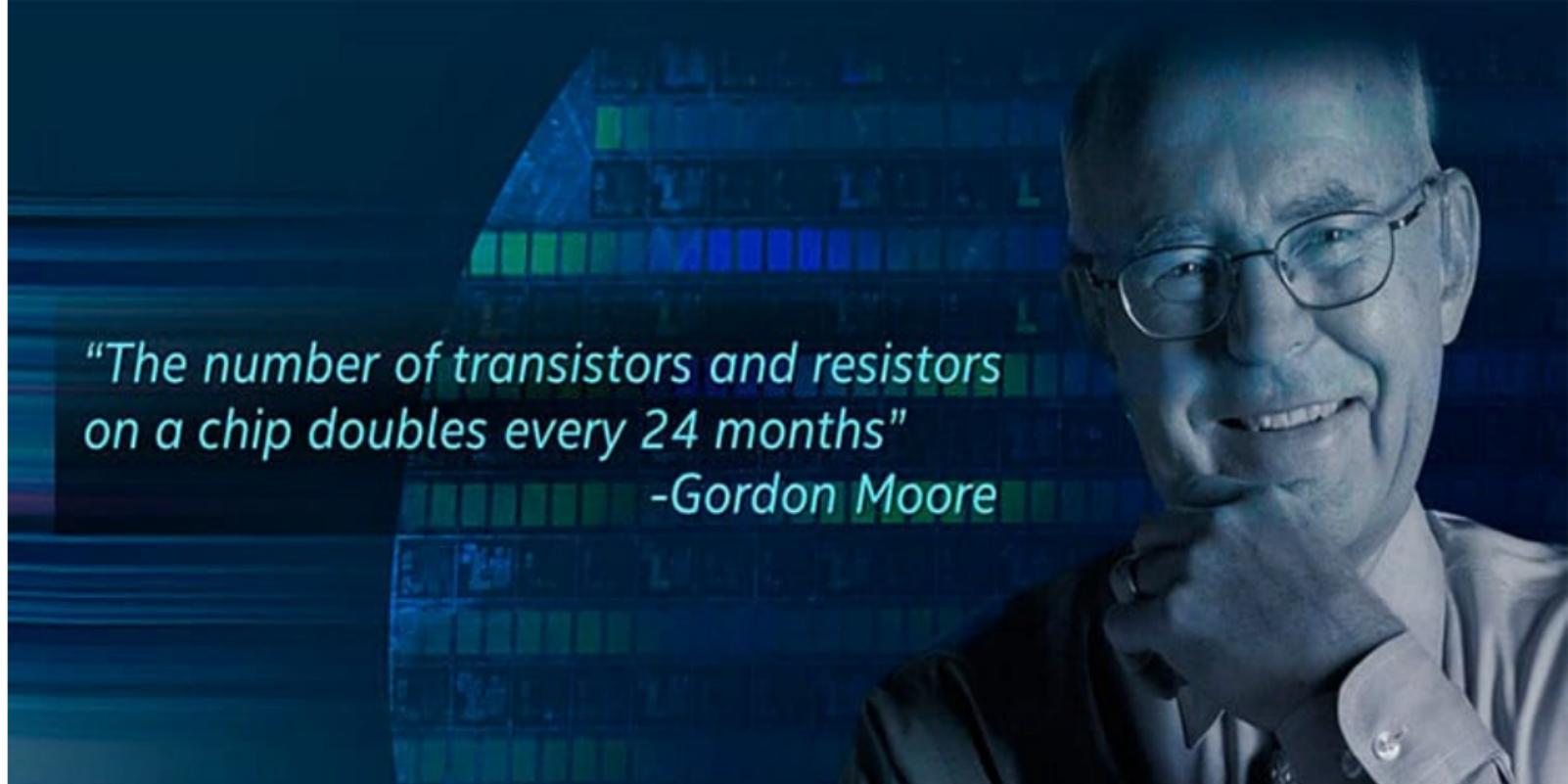
q: 0 |0> H S  
q: 1 |0> H + X  
q: 2 |0>  
+  
c3

Probabilities

Computational basis states	Probability (%)
000	~25
001	~25
010	0
011	0
100	~25
101	~25
110	0
111	0

Q-sphere

# Lei de Moore

A portrait of Gordon Moore, co-founder of Intel, wearing glasses and a light-colored shirt, smiling. He is positioned on the right side of the slide. In the background, there is a large, glowing blue computer chip with various electronic components and circuit patterns.

*"The number of transistors and resistors  
on a chip doubles every 24 months"*

-Gordon Moore

# Lei de Moore - Consequências

Quantos qubits o maior supercomputador consegue simular?

- Limite atual - 45 - 50 qubits
- 40 qubits precisa de 9 TB
- 50 qubits precisa de 9 PB
- IBM Q Yorktown (5 qubits)

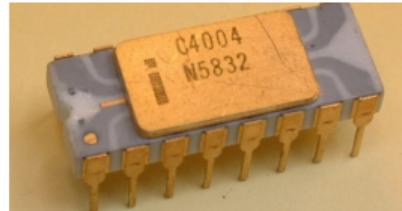


Figure: Intel 4004- 2300 componentes eletrônicos (1971)



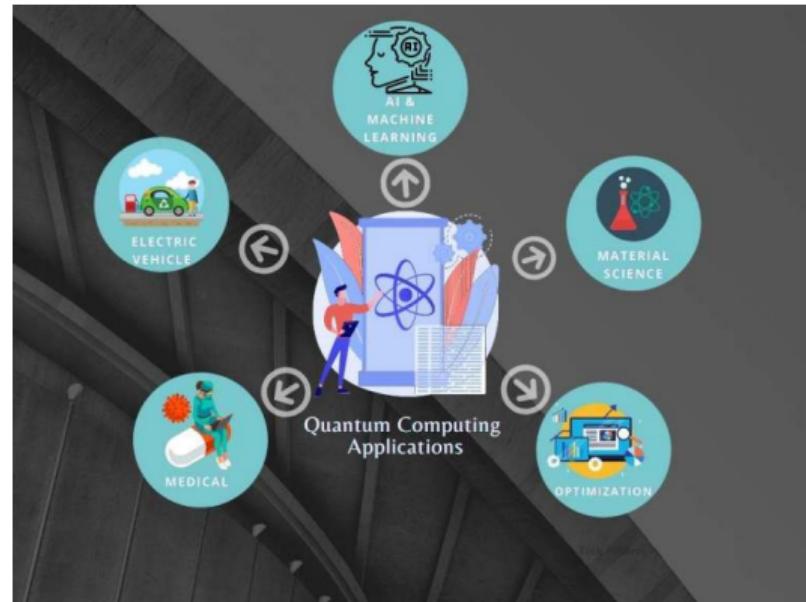
Figure: Verificar a quantidade de componentes eletrônicos

# A História da Computação Quântica

- 1980 - P. Benioff e Y. Manin em Russo
- 1981 - R. Feynman - Um CC não consegue simular eficientemente a MQ
- 1985 - D. Deutsch - Máquina de Turing Quântica
- 1992 - D. Deutsch - Modelo de circuitos
- 1994 - Algoritmo de Shor
- 1995 - P. Shor - Código Quântico de Correção de Erros
- 1996 - Algoritmo de Grover
- 2001 - Fatoração de 15 com 7 qubits (RMN)
- 2006 - IQC, PI, MIT desenvolvem um CQ de 12 qubits
- 2011 - D-Wave faz CQA de 128 qubits
- 2017 - IBM disponibiliza CQ de 16 qubits de uso público
- 2019 - Supremacia quântica pela Google

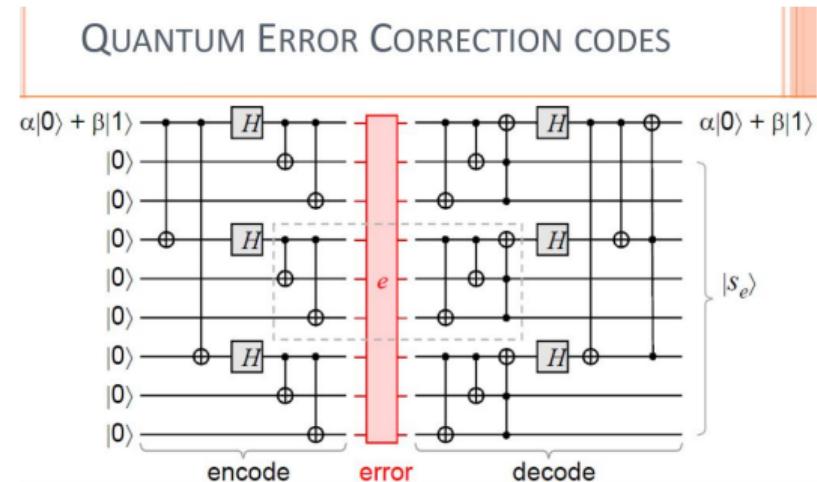
# Onde usar o CQ?

- Machine Learning
- Otimização
- Biologia Molecular
- Telecomunicações
- Serviços Financeiros
- Criptografia
- Problemas de Busca
- Equações Diferenciais



# Códigos quânticos corretores de erros

- Uso obrigatório
- Redundância: 1 qubit  $\rightarrow$  5 qubits
- Limiar de erro baixíssimo: entre  $10^{-6}$  e  $10^{-2}$
- Probabilidade de erro diminui de forma quadrática.



# Algoritmos Quânticos

- Principais Algoritmos:
  - Shor(1994)
  - Grover (1996)
  - Element distinctness (2004)
  - HHL (2009)
- Principais Técnicas
  - Amplificação de amplitude
  - Transformada de Fourier
  - Passeios quânticos
  - QAOA
  - VQE
  - Annealing

# Leis da MQ - as regras do jogo!

- ① O estado de um sistema físico isolado é uma superposição de possíveis estados (vetores) deste sistema.
- ② A evolução do sistema é descrita pela aplicação de um operador unitário ao vetor que descreve o estado do sistema.
- ③ Uma medição colapsa a superposição para uma única possibilidade clássica.
- ④ O estado de sistemas compostos é obtido via produto das partes.

# Postulados da MQ - Espaço de Estados

Um sistema físico isolado está associado a um espaço de Hilbert, chamado espaço de estados. O estado do sistema é totalmente descrito por um vetor unitário, chamado vetor de estado neste espaço.

Um estado genérico de 1 qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

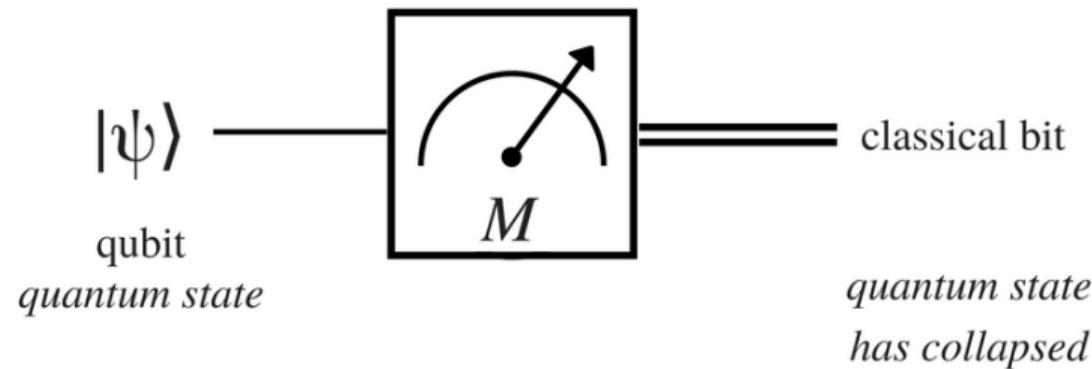
Onde

$$|\alpha|^2 + |\beta|^2 = 1.$$

Os estados quânticos  $|0\rangle$  e  $|1\rangle$  são descritos por

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

# Postulados da MQ - Medida



- Estado antes da medida:  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Estado após a medida:  $|0\rangle$  com prob.  $|\alpha|^2$  ou  $|1\rangle$  com prob.  $|\beta|^2$

# Notação de Dirac

- $v \rightarrow |v\rangle$

- Base:

$$\{v_0, v_1, \dots, v_{n-1}\} \rightarrow \{|v_0\rangle, |v_1\rangle, |v_n\rangle\} \rightarrow \{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$$

- **Importante:** Vetor  $|0\rangle \neq$  vetor nulo.

- Vetor com  $n$  entradas:  $|v\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$

- Vetor dual:  $\langle v| = [a_1^*, a_2^*, \dots, a_n^*]$

# Notação de Dirac

- Produto interno:  $\langle s | s \rangle \sum_{i=1}^n a_i^* a_i$
- Base ortonormal:  $\langle s | s \rangle = \delta_{ij}$
- Produto externo:

$$|s\rangle \langle s| = \begin{bmatrix} a_1 a_1^* & \dots & a_1 a_n^* \\ & \ddots & \\ a_n a_1^* & \dots & a_n a_n^* \end{bmatrix}$$

# Circuitos Quânticos

Um circuito quântico é uma coleção de portas quânticas (matrizes unitárias) interconectadas por fios e são utilizados para executar tarefas no computador quântico.

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$$

Onde

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

# Matrizes de Pauli

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

# Produto Tensorial - Estado de dois qubits

- Estados de 1 qubit da base computacional

$$|1\rangle \otimes |0\rangle = |10\rangle = |2\rangle$$

- Para estados genéricos  $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$  e  $|\psi_2\rangle = \alpha'|0\rangle + \beta'|1\rangle$  temos

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_2\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle) \\ &= \alpha\alpha'|0\rangle + \alpha\beta'|1\rangle + \beta\alpha'|2\rangle + \beta\beta'|3\rangle \end{aligned}$$

## Base computacional - 2 qubits

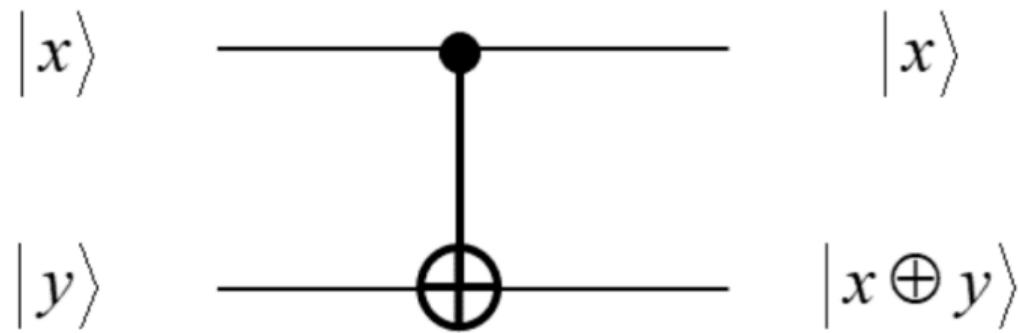
$$|0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|1\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|2\rangle = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|3\rangle = |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

## Porta CNOT - 2 qubits

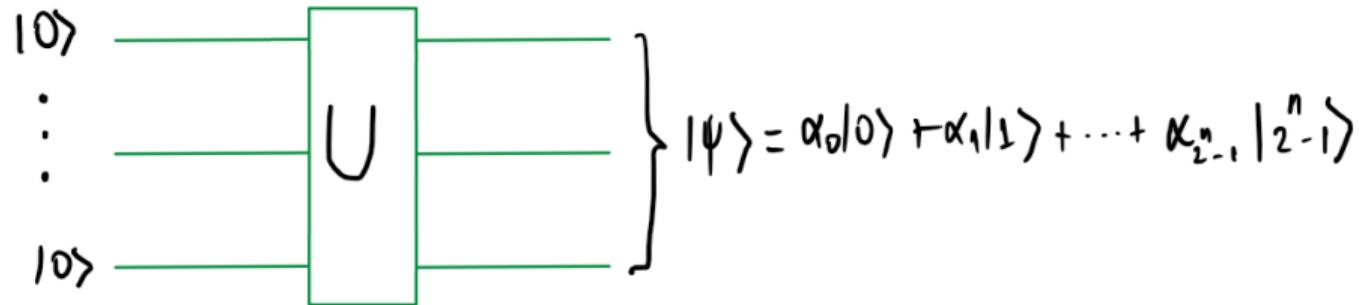


## Base computacional - n qubits

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \dots \quad |N-1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

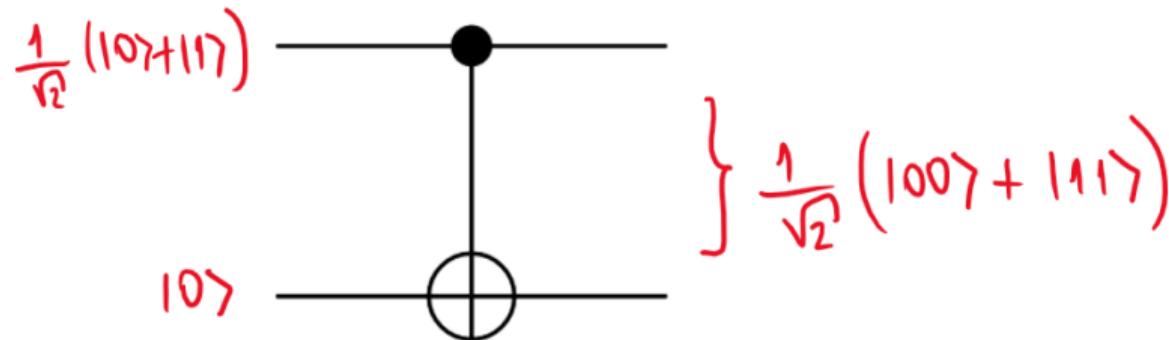
Onde  $N = 2^n$ ,  $n$  é o número de qubits.

# Modelo padrão da computação quântica



- A porta  $U$  deve satisfazer  $UU^\dagger = I$
- Realize uma medição na base computacional
- Obtenha o estado  $|i\rangle$  com probabilidade  $|\alpha_i|^2$

# Criando emaranhamento

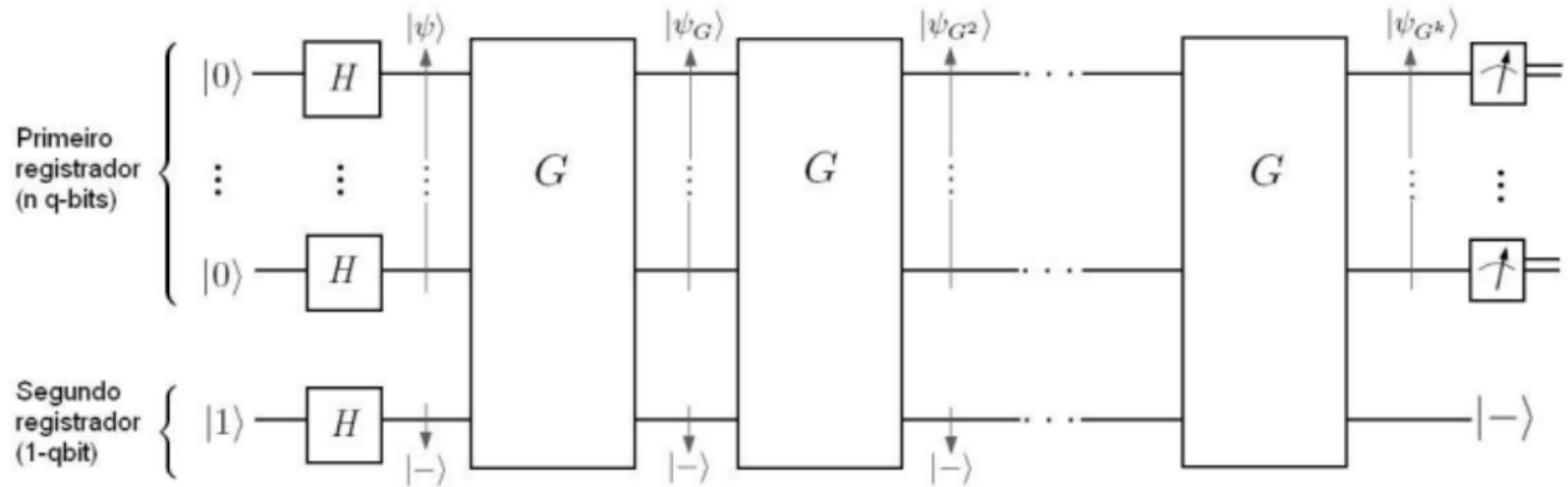


- Após uma operação de medida, o resultado é
  - $|00\rangle$  com probabilidade  $\frac{1}{2}$
  - $|11\rangle$  com probabilidade  $\frac{1}{2}$

# O algoritmo de Grover - Objetivo

- **Objetivo:** Seja  $X = \{x_1, x_2, \dots, x_N\}$  um conjunto com  $N$  elementos não ordenados. Dada uma função  $f : X \rightarrow \{0, 1\}$ , o objetivo é encontrar elemento  $x_p$  em  $X$  tal que  $f(x_p) = 1$ .
- O algoritmo de Grover necessita apenas de  $O(\sqrt{N})$  operações.

# O algoritmo de Grover - Circuito



# O algoritmo de Grover - Inicializando

- Obs.:  $2^n = N$  elementos,  $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  e  $x_p$  é o elemento procurado.
- 1º registrador: sistema com  $n$  qubits inicialmente no estado  $|0\rangle = |0\rangle^{\otimes n}$ .

$$\{|0\rangle, |1\rangle, \dots, |x_p\rangle, \dots, |N-1\rangle\}$$

$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} |0\rangle + \dots + \frac{1}{\sqrt{N}} |N-1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2º registrador: sistema com 1 qubit inicialmente no estado  $|1\rangle$ .

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

# O algoritmo de Grover - O oráculo

- O oráculo:

$$f(x) = \begin{cases} 1, & x = x_p \\ 0, & x \neq x_p \end{cases}$$

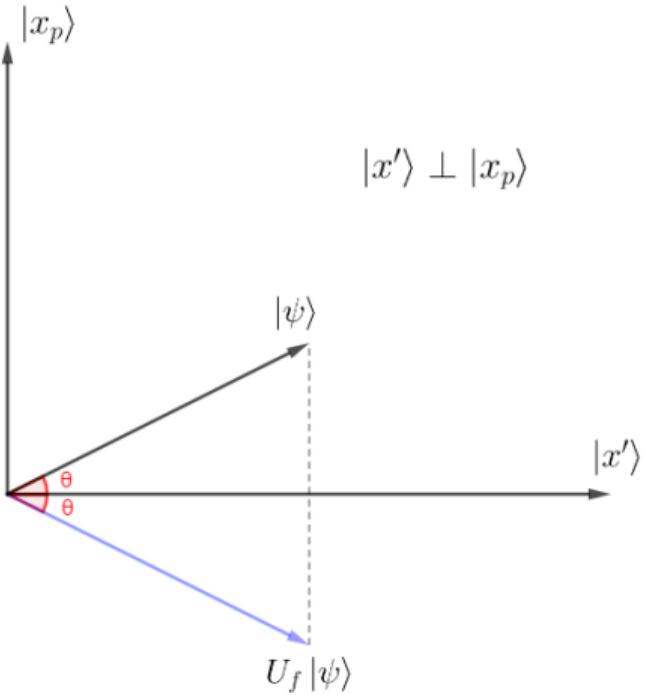
- Marcando o elemento procurado:

**Definição:**  $U_f |a\rangle |b\rangle = |a\rangle |b \oplus f(x)\rangle$ , onde  $\oplus$  representa a soma módulo 2.

$$U_f |x\rangle |- \rangle = (-1)^{f(x)} |x\rangle |- \rangle$$

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

$$U_f |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(x)} |x\rangle = |\psi_1\rangle$$



Dedução:

$$U_f |x\rangle |- \rangle = \frac{1}{\sqrt{2}}(U_f |x\rangle |0\rangle - U_f |x\rangle |1\rangle)$$

$$U_f |x\rangle |- \rangle = \frac{1}{\sqrt{2}}(|x\rangle |0 + f(x)\rangle - |x\rangle |1 + f(x)\rangle)$$

$$U_f |x\rangle |- \rangle = \begin{cases} \frac{1}{\sqrt{2}}(|x\rangle |1\rangle - |x\rangle |0\rangle), & x = x_p \\ \frac{1}{\sqrt{2}}(|x\rangle |0\rangle - |x\rangle |1\rangle), & x \neq x_p \end{cases}$$

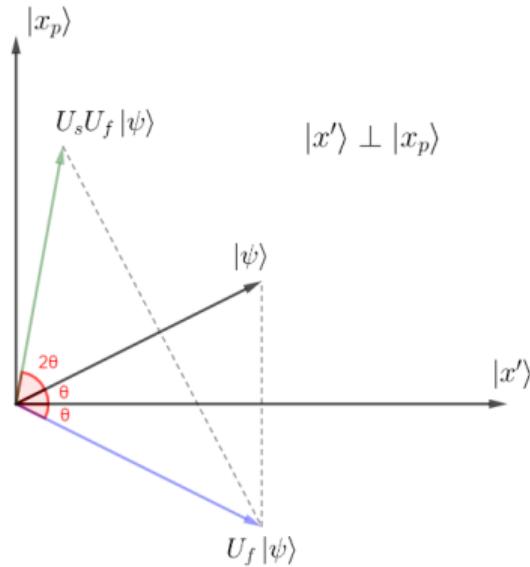
$$U_f |x\rangle |- \rangle = (-1)^{f(x)} |x\rangle |- \rangle$$

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

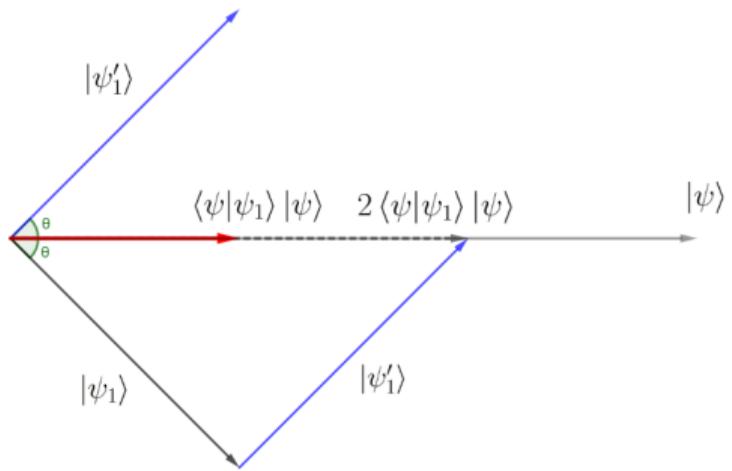
# O operador de difusão $U_s$

- Amplificando o elemento marcado:

**Definição:**  $U_s = (2 |\psi\rangle\langle\psi| - I)$  e  $U_s |\psi_1\rangle = |\psi_2\rangle$ .



Dedução:



$$|\psi'_1\rangle + |\psi_1\rangle = 2\langle\psi|\psi_1\rangle|\psi\rangle$$

$$|\psi'_1\rangle = 2\langle\psi|\psi_1\rangle|\psi\rangle - |\psi_1\rangle$$

$$|\psi'_1\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle$$

$$U_s = (2|\psi\rangle\langle\psi| - I)$$

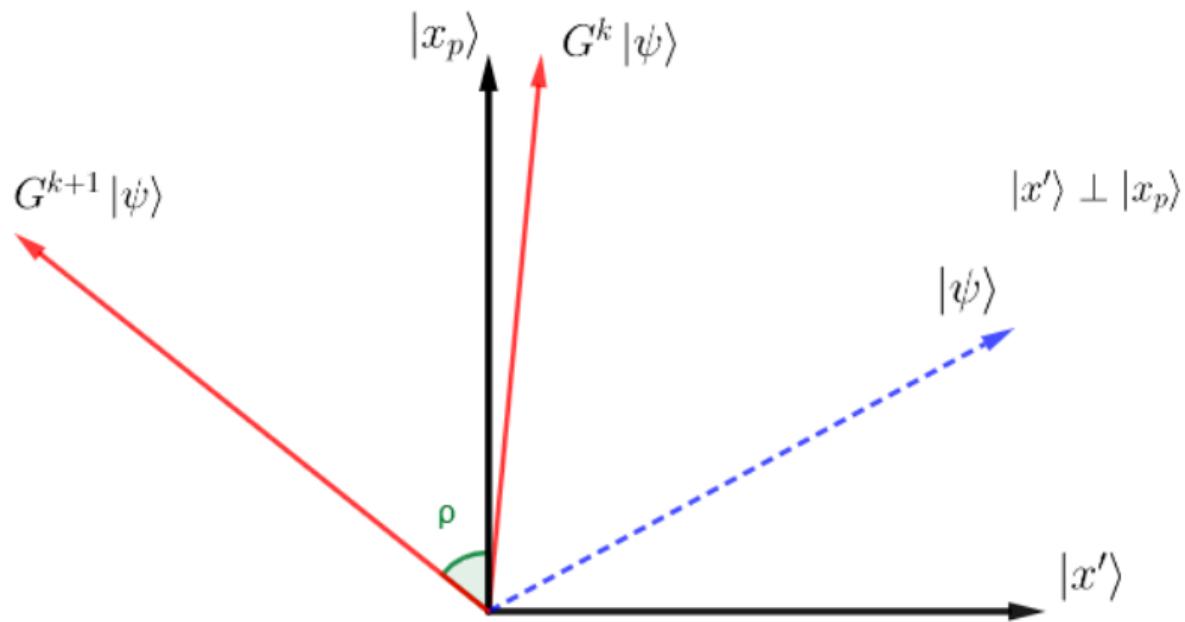
# O operador de Grover $G$

**Definição:**  $G |\psi\rangle = U_s U_f |\psi\rangle$ , ou seja,  $G = U_s U_f$ .

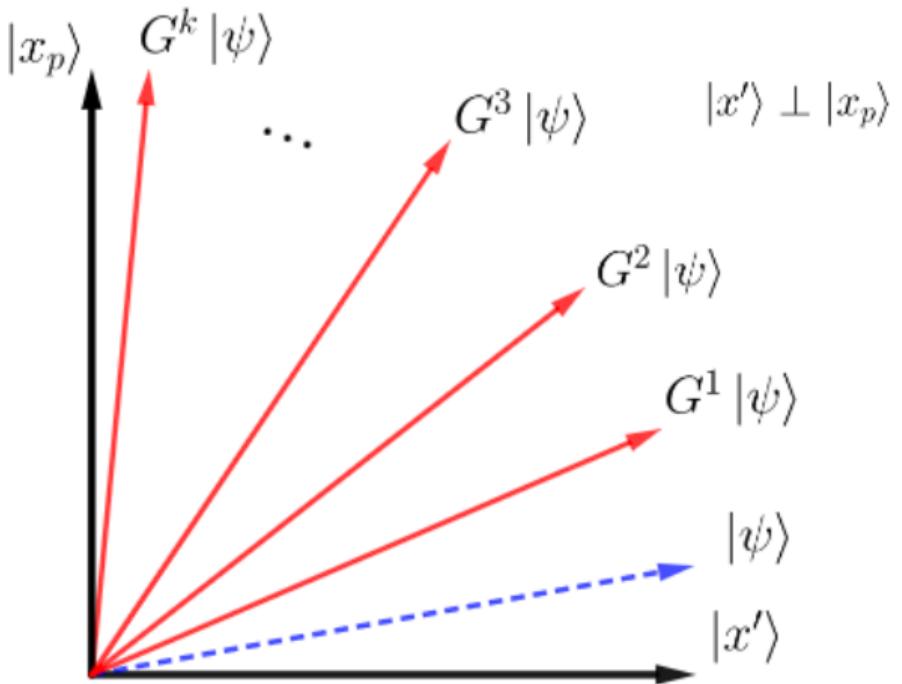
$G$  deve ser aplicado  $k$  vezes para uma aproximação satisfatória.



Quanto vale  $k$ ?



$$k = \frac{\pi}{4}\sqrt{N}$$



# Resumindo...

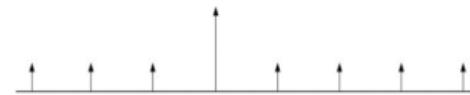
- Aplicando  $H$ :



- Operador  $U_f$ :



- Operador  $U_s$ :



- Medição: Colapsar para  $|x_p\rangle$  com uma probabilidade associada.

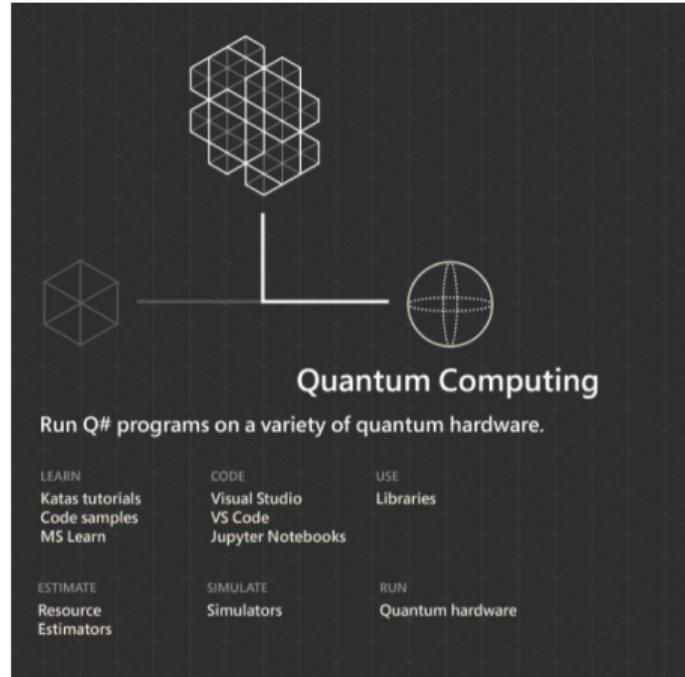
# Aula 3: Computadores Quânticos

## Principais Projetos de Desenvolvimento:

- IBM Quantum Computing (Qiskit);
- Microsoft Azure Quantum (Q);
- Google AI (Cirq).

# Microsoft Azure Quantum

Iniciativa da Microsoft para simulação e desenvolvimento de algoritmos quânticos



## Iniciativa da Google para simulação e desenvolvimento de algoritmos/circuitos quânticos

The screenshot displays the Google Quantum Computing website, featuring several key components:

- Cirq (Framework):** A Python library for writing, manipulating, and optimizing quantum circuits and running them against quantum computers and simulators. It includes a "Learn more" button.
- OpenFermion (Library):** An open source library for compiling and analyzing quantum algorithms to simulate fermionic systems, including quantum chemistry. It includes a "Learn more" button.
- TensorFlow Quantum (Library):** An open source library for hybrid quantum-classical machine learning. It includes a "Learn more" button.
- Quantum Computing Service:** Provides remote access to Google's world-leading quantum processors and simulators. It includes a "Learn more" button and a photograph of a complex quantum computing hardware setup.
- Hardware overview:** Details of leading quantum hardware and types of experiments. It includes a "Learn more" button and a photograph of a blue and orange quantum processor chip.
- Hardware specifications:** Performance and functionality of latest quantum processors. It includes a "View the datasheet" button and a photograph of a gold-colored quantum processor chip.

# IBM Quantum Computing

## Iniciativa da IBM para simulação e desenvolvimento de algoritmos/circuitos quânticos

### IBM Quantum solutions

IBM's full-stack approach delivers the best of IBM's quantum computing systems together with the most complete suite of quantum software tools and cloud services.

#### IBM Quantum Services

IBM Quantum Services offer access to the latest, world-leading quantum systems, simulators, runtimes and programming tools, all through the IBM Cloud.

[View IBM Quantum Services](#)



#### Systems & Simulators

Our 20+ quantum systems make up the most powerful fleet of quantum computers in the world, with every level of machine based on Quantum System One technology.

[View Quantum Systems](#)



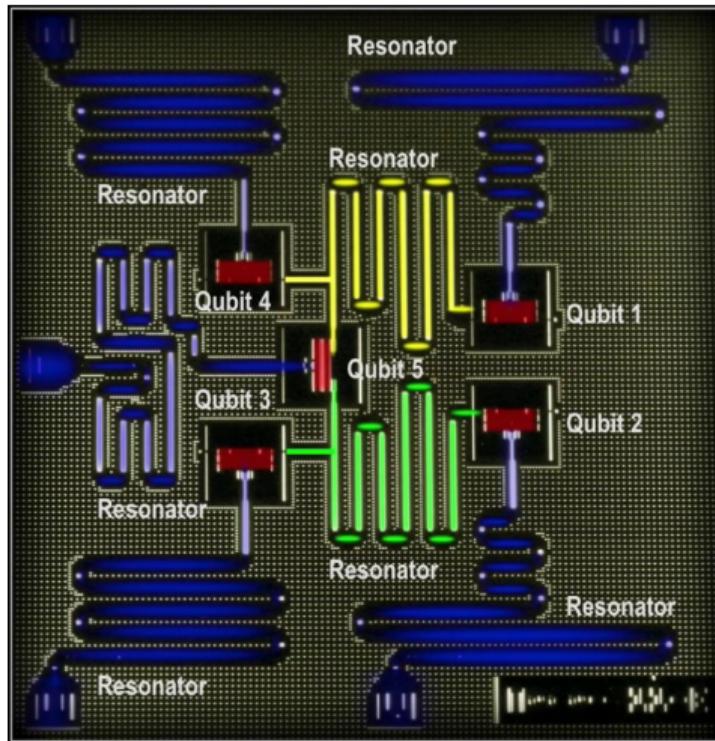
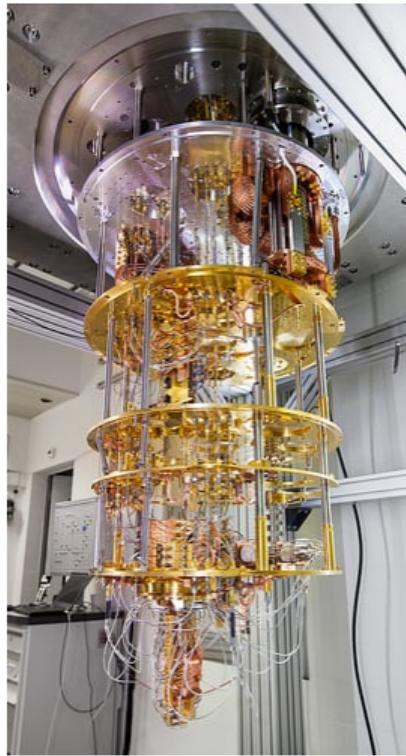
#### Tools & Software

Visually build quantum circuits in IBM Quantum Composer to run on real quantum systems. Or prototype applications on the cloud with IBM Quantum Lab. It's all powered by Qiskit, IBM's open-source SDK.

[View all tools](#)



# Hardware Quântico - IBM



**IBM's 5-Qubit Processor**

Legend:

- Bus Resonator (Green)
- Control and Read-out Resonator (Yellow)
- Qubit (Blue)

# Hardware Quântico - IBM

# Aula 4: Grover's QSA

## Esquema:

- DS-CDMA (Direct-Sequencence Code Division Multiple Access), com  $K = 2$  usuários;
- Modulação BPSK com  $M = 2$  estados;
- Os coeficientes do canal são assumidos serem estimados perfeitamente;
- A função custo original  $f(x) = P(y|x) = \exp(-\|y - Rx\|^2/2\sigma^2)$  será trocada por  $f : \{0, 1, 2, 3\} \rightarrow [0, 1]$ , com espaço de busca  $N = M^K = 4$ .
- Assuma que a função custo resulta

$$[f(0), (f(1), f(2), f(3))] = [0.24, 0.16, 0.38, 0.27]$$

que representa a probabilidade  $P(y|x)$  de receber um sinal  $y$  dado que um sinal  $x$  foi transmitido.

# Grover's QSA

Assuma que o elemento procurado seja  $x_0 = 2$  tal que  $f(x_0) = 0.38$ :

**Passo 1.** Inicialize o CQ no estado  $|0, 0\rangle$  e aplique  $H^{\otimes 2}$ :

$$|\psi_1\rangle = \frac{1}{\sqrt{4}} \sum_{q=0}^{2^2-1} |q\rangle = \frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle \frac{1}{2} |2\rangle + \frac{1}{2} |3\rangle$$

Defina o operador unitário,  $U_g$ , tal que

$$U_g(|x\rangle |w\rangle) = |x\rangle |w \oplus g(x)\rangle,$$

onde

$$g(x) = \begin{cases} 1 & \text{se } f(x) = 0.38 \\ 0 & \text{caso contrário.} \end{cases}$$

# Grover's QSA

No nosso cenário, temos:

$$g(x) = \begin{cases} 0, & \text{se } x = 0, \text{ pois, } f(0) = 0.24 \neq 0.38 \\ 0, & \text{se } x = 1, \text{ pois, } f(1) = 0.16 \neq 0.38 \\ 1, & \text{se } x = 2, \text{ pois, } f(2) = 0.38 \\ 0, & \text{se } x = 3, \text{ pois, } f(3) = 0.27 \neq 0.38 \end{cases}$$

Note também que

$$U_g(|x\rangle |-\rangle) = (-1)^{g(x)} |x\rangle |-\rangle.$$

# Grover's QSA

**Passo 2.** Aplique o operador  $U_g$  ao estado  $|\psi_1\rangle|-\rangle$ :

$$\begin{aligned} |\psi_2\rangle &= \left( \frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle - \frac{1}{2} |2\rangle + \frac{1}{2} |3\rangle \right) |-\rangle \\ &= \left( |\psi_1\rangle - \frac{2}{\sqrt{2^2}} |2\rangle \right) |-\rangle. \end{aligned}$$

Note que

$$\langle\psi_1|2\rangle = \frac{1}{\sqrt{2^2}}$$

# Grover's QSA

**Passo 3.** Aplique o operador de Grover  $G = (2|\psi_1\rangle\langle\psi_1| - I)$  ao estado  $|\psi_2\rangle$ :

$$\begin{aligned} |\psi_3\rangle &= (2|\psi_1\rangle\langle\psi_1| - I)|\psi_2\rangle \\ &= \frac{2^{2-2}-1}{2^{2-2}}|\psi_1\rangle + \frac{2}{\sqrt{2^2}}|2\rangle. \\ &= 0.|0\rangle + 0.|1\rangle + 1.|2\rangle + 0.|3\rangle \end{aligned}$$