



# Historia y futuro de la computación cuántica

Barbara Candia

Organizadora

Santiago, enero 2025

# Estructura de la presentación

- 1 Introducción a la era de la computación Cuántica
- 2 Primeras propuestas de algoritmos cuánticos
- 3 Nuevos algoritmos y computadores cuánticos actuales (NISQ)
- 4 El futuro de la computación cuántica

# La visión de Richard Feynman

En 1982 la historia de la computación cuántica comienza con las conferencias de Richard Feynman.

- *Simulating physics with computers*: Una visión más abstracta sobre la programación en la física y lo que se necesita para abordar la simulación de efectos cuánticos.
- *Quantum mechanical computers*: Se centra en más detalles sobre cómo funcionaría una computadora cuántica y cómo se diseñarían los algoritmos cuánticos

# Computadora cuántica universal

En 1985 David Deutsch publica la idea de una “computadora cuántica universal”, potenciando el principio de Church-Turing.

- Un dispositivo informático universal puede simular todos los procesos físicos.
- Algoritmo de Deutsch: Resuelve un problema sencillo conocido como la “determinación de funciones constantes” utilizando solo una evaluación.

# Algoritmo de Shor

En 1994 Peter Shor presenta un algoritmo que puede encontrar eficientemente los factores de números grandes, superando significativamente al mejor algoritmo clásico.

- Se basa en la capacidad de las computadoras cuánticas para aprovechar la superposición y el entrelazamiento cuántico
- Esto lo hace revolucionario para la seguridad de datos, ya que pone en riesgo los sistemas de encriptación actuales.

# Criptografía cuántica

Gracias al impacto del algoritmo de Shor, comenzó una sucesión de hitos que marcaron el inicio de la conocida era de la computación cuántica

- Generación de interés científico y político gracias a la *amenaza* a la criptografía clásica.
- Inicio del estudio para generar protocolos cuánticos seguros (QKD) como el protocolo BB84.
- Fomento a la innovación en *hardware cuántico*.

# Simulación cuántica

En 1990 se desarrollaron los primeros algoritmos teóricos para simulaciones cuánticas, tras décadas de trabajo se pueden destacar resultados como:

- Modelos de Ising y Magnetismo Cuántico
- Simulación de Reacciones Químicas
- Dinámicas cuánticas fuera del equilibrio
- Física de altas energías

## Y muchos aportes mas..

1996: Lov Grover presenta un algoritmo para computadoras cuánticas que sería más eficiente para búsquedas en bases de datos (algoritmo de búsqueda de Grove)

1996: Seth Lloyd propone un algoritmo cuántico que puede simular sistemas mecánicos cuánticos.

1999: Geordie Rose funda D-Wave Systems



# Cirac y Zoller: Computación cuántica de iones

Propusieron un modelo para implementar un computador cuántico basado en iones atrapados, que todavía es uno de los enfoques más prometedores para construir computadoras cuánticas.

- Uso de iones atrapados como qubits.
- Manipulación de estados cuánticos
- Acoplamiento mediante el modo vibracional
- Corrección de errores cuánticos

## Y muchos muchos aportes mas...

2000: Eddie Farhi en el MIT desarrolla la idea de la computación cuántica adiabática

2001: IBM y la Universidad de Stanford publican la primera implementación del algoritmo de Shor, factorizando 15 en sus factores primos en un procesador de 7 qubits.

2010: D-Wave One, se lanza el primer ordenador cuántico comercial (annealer)

# IBM Quantum System one

Es uno de los primeros sistemas de computación cuántica completamente integrados, escalables y accesibles desarrollados por IBM.

- Procesador cuántico
- Diseño integrado
- Interfaz de acceso
- Ruido y errores

# Video en Beamer

# Computadores cuánticos NISQ

Son capaces de operar con un número moderado de qubits, pero todavía están limitados por el ruido, la decoherencia y otros errores.

- Tienen entre 50 y 1000 qubits.
- Pueden complementar los algoritmos clásicos mediante un enfoque híbrido
- Tienen un gran potencial en tareas como la optimización, simulación y aprendizaje automático.

# Algoritmos variacionales

Representan un enfoque híbrido que combina la computación cuántica con métodos clásicos para resolver problemas complejos.

- *Variational Quantum Eigensolver (VQE)*
- *Quantum Approximate Optimization Algorithm (QAOA)*
- *Quantum Neural Networks (QNNs)*
- *Adaptative Variational Quantum Solver (ADAPT-VQE)*

# Logros y desafíos

- Implementaciones experimentales
- Aplicaciones diversificadas
- Mejoras en la eficiencia

- Ruido y decoherencia
- Optimización clásica
- Barreras de desvanecimiento del gradiente

# Machine learning cuántico

Busca aprovechar las propiedades cuánticas como la superposición, el entrelazamiento y la interferencia para resolver problemas de aprendizaje de manera más eficiente.

- Algoritmo de Harrow, Hassidim y Lloyd (HHL)
- *Quantum Support Vector Machines (QSVM)*
- *Quantum Principal Component Analysis (QPCA)*
- *Quantum Neural Networks (QNNs)*



# Promesas y desafíos

- Reducción del tiempo de cálculo
- Eficiencia en dimensiones altas
- Aprendizaje con datos limitados

- Hardware limitado
- Escalabilidad
- Integrabilidad
- Falta de ventaja práctica

# Computación *fault tolerant* y corrección de errores

Capacidad de un sistema cuántico de continuar funcionando correctamente a pesar de errores o fallos en el hardware cuántico, como la decoherencia y la interferencia.

- Códigos de corrección de errores cuánticos
- Fidelidad en compuertas cuánticas
- Tolerancia a fallos mediante qubits topológicos

# El siguiente paso de los computadores NISQ

## Corrección de Errores Cuánticos

- Para alcanzar la computación cuántica a gran escala, será crucial implementar códigos de corrección de errores que compensen la decoherencia y el ruido.

## Escalabilidad del Hardware

- Ampliar el número de qubits y mejorar su conectividad y fidelidad.
- Desarrollar tecnologías más allá de los qubits superconductores y de iones atrapados, como los qubits topológicos.

# El futuro en la industria

IBM, D-wave systems, Microsoft y Google planean avanzar hacia sistemas cuánticos más potentes y escalables.

- 2024 IBM Condor: Primer procesador cuántico universal con más de 1.000 qubits.
- 2025 Procesadores cuánticos modulares: Sistemas en red que permitirán alcanzar configuraciones de más de 4.000 qubits.
- 2033 Super-computadores Cuánticos: Sistemas capaces de ejecutar un billon de compuertas lógicas en sistemas de 2.000 qubits.

# En resumen, ¿que esperamos de la computación cuántica?

Química cuántica y diseño de materiales: Modelar materiales y sistemas moleculares complejos.

- Calcular con precisión las propiedades de moléculas complejas para diseñar nuevos materiales.
- Optimizar procesos químicos como la producción de baterías más eficientes.
- Descubrir nuevos medicamentos mediante simulaciones moleculares detalladas.

## Optimización Combinatoria

- Resolver problemas NP-complejos en logística, planificación y diseño urbano.
- Mejorar algoritmos de optimización utilizados en industrias como finanzas y transporte.

## Machine Learning Cuántico

- Procesar grandes cantidades de datos con una ventaja exponencial en ciertas tareas.
- Mejorar modelos de aprendizaje automático en áreas como reconocimiento de patrones, análisis de datos y predicción.

## Seguridad y Criptografía

- Desarrollar métodos de encriptación post-cuánticos para proteger datos frente a ataques.
- Implementar sistemas de comunicación cuántica completamente seguros basados en el entrelazamiento y la distribución de claves cuánticas.

## Simulación de Sistemas Físicos Complejos

- Avanzar en la comprensión de fenómenos fundamentales en física.
- Desarrollar tecnologías avanzadas como reactores de fusión o materiales superconductores a temperatura ambiente.

## Ciencias Biológicas y Medicina

- Diseñar terapias personalizadas mediante simulaciones detalladas del ADN y proteínas.
- Optimizar ensayos clínicos y acelerar el descubrimiento de medicamentos.

## Análisis Financiero

- Mejorar la precisión de modelos de riesgo y portafolios financieros.
- Optimizar mercados financieros y sistemas de negociación.



# Bibliografía

