Curso de Computación Cuántica

Algorítmica y Software

Joaquín Keller

2025 UCV

Algorítmica y Software

~~Hardware cuántico~~, ~~física cuántica~~

Bases matemáticas (álgebra de tensores, TCS, . . .)

Algoritmos cuánticos: estudio, diseño, implementación

Herramientas de software (Mathematica™, LaTeX, Qiskit, . . .)

Clases de complejidad algorítmica

P = problemas que se pueden resolver en tiempo **polinomial**,
con una **máquina clásica de Turing**

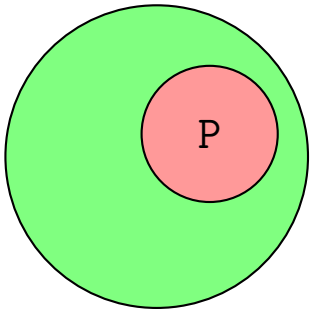
BQP (Bounded-error Quantum Polynomial time) =
problemas que se pueden resolver en tiempo **polinomial**
con una **máquina cuántica de Turing**

polinómico o polinomial: $O(n^k)$, n es el tamaño del problema

Ventaja cuántica

$\mathtt{P} \subseteq \mathtt{BQP}$

$\mathtt{BQP} \neq \mathtt{P}$ (conjetura)



BQP

$\mathtt{BQP} - \mathtt{P}$ = ventaja cuántica

Ejemplo de ventaja cuántica: el algoritmo de Shor

Algoritmo de Shor

Problema: conseguir los factores primos de N

Algoritmo cuántico de Shor: $\boxed{O(n^2 log\, n) < O(n^3)}$ es decir polinomial

n: numero de dígitos de N $\quad n = log\, N$

El mejor algoritmo clásico *conocido* es GNFS y es super-polinomial

GNFS: $\boxed{O(e^{c\sqrt[3]{n\, log^2 n}})}$ $\quad c = \frac{1}{3}\sqrt[3]{92 + 26\sqrt{13}} = 1.901883...$

Conjetura: no existe un algoritmo clásico **polinomial** para ese problema

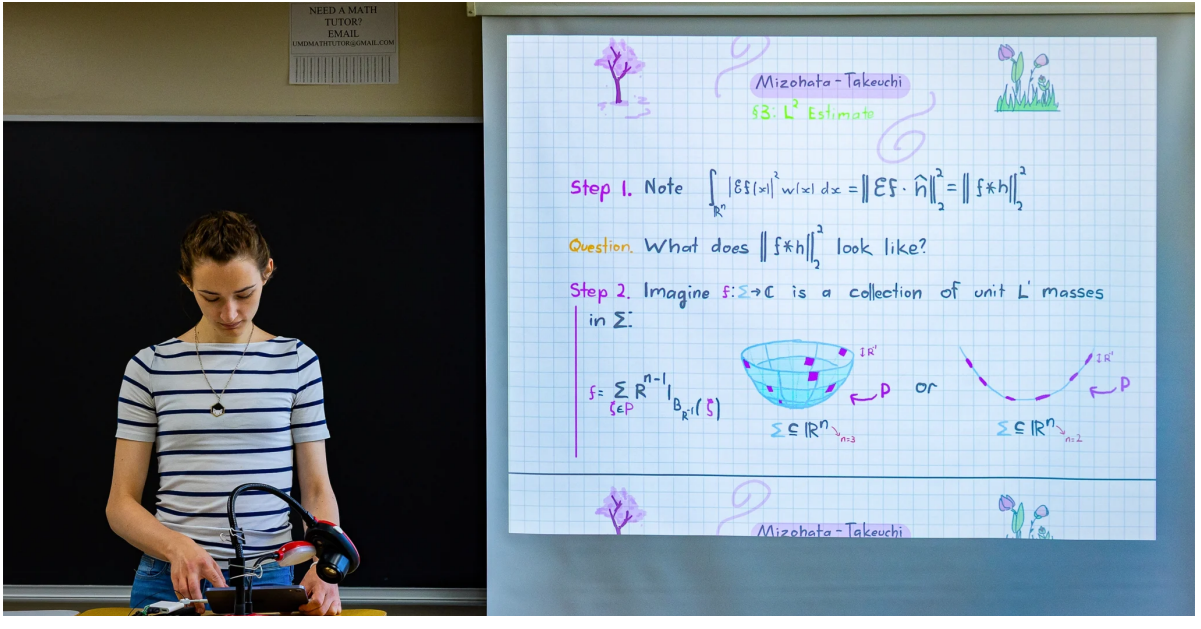
Conjeturas

- Gran teorema de Fermat (1637): para todo n entero $n > 2$
la ecuación $x^n + y^n = z^n$ no tiene soluciones en enteros no nulos
Demostración en 1995 por Andrew Wiles

- Goldbach (1742): todo número par > 2 es suma de dos primos
- $P \neq NP$ (1971)
Sin demostrar en 2025

- Mizohata-Takeuchi (1984)
Hannah Cairo demuestra en 2025 que es falsa

Hannah Cairo, 17 años, nativa de Bahamas

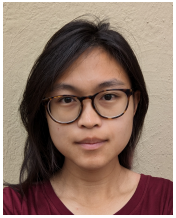


Algoritmo de Kerenidis–Prakash

2016: Kerenidis y Prakash diseñan un algoritmo cuántico para un problema de machine learning que es exponencialmente más rápido que el mejor algoritmo clásico *conocido*

Algoritmo de Kerenidis–Prakash

2016: Kerenidis y Prakash diseñan un algoritmo cuántico para un problema de machine learning que es exponencialmente más rápido que el mejor algoritmo clásico *conocido*



2018: Ewing Tang, 17 años, diseña un algoritmo clásico que es igual de rápido. El algoritmo de Kerenidis–Prakash pierde su ventaja cuántica...

Ventaja cuantica del algoritmo de Shor

Problema primfact : conseguir los factores primos de N

1. Existe un algoritmo cuántico polinomial: primfact $\in$ BQP
2. No hay algoritmo clásico polinomial: primfact $\notin$ P

primfact $\notin$ P es una conjetura, i.e. sin demostrar

La ventaja cuantica del algoritmo de Shor es una conjetura

Una conjetura sólida?

Test de primalidad

Problema: es N primo?

2002: Algoritmo polinomial de Agrawal, Kayal, Saxena

El algoritmo AKS no fue una sorpresa...

1975: Primeros elementos indicando que podía ser polinomial

1980: Algoritmo de Miller-Rabin de tiempo polinomial
con una demostración parcial, que depende de la hipótesis de Riemann (conjetura muy sólida)

La conjetura $\mathtt{P} \subset \mathtt{BQP}$ es sólida

Porque si fuera falsa, muchas otras conjeturas serían falsas también

La conjetura en español: 'existen algoritmos con ventaja cuántica'

Menos mal porque sino la computación cuántica no tendría utilidad

Problema 1: conocemos pocos algoritmos con ventaja cuántica

Problema 2: no tenemos ningún algoritmo con valor económico

El algoritmo de Shor no tiene valor económico

El algoritmo de Shor permite romper la criptografía RSA
Valor económico solo para espías y delincuentes

La criptografía RSA va a desaparecer de aquí a 2030
remplazada por la criptografía post-cuántica

Valor residual: algunas comunicaciones encriptadas con RSA se están guardando para ser desencriptadas en el futuro

Ventaja cuántica en química ?

nature communications

Article

https://doi.org/10.1038/s41467-023-37587-6

Evaluating the evidence for exponential quantum advantage in ground-state quantum chemistry

Received: 31 January 2023

Accepted: 22 March 2023

Published online: 07 April 2023

Seunghoon Lee[1], Joonho Lee[2], Huanchen Zhai[1], Yu Tong[3], Alexander M. Dalzell[4], Ashutosh Kumar[5,6], Phillip Helms[1], Johnnie Gray[1], Zhi-Hao Cui[1], Wenyuan Liu[1], Michael Kastoryano[4,7], Ryan Babbush[8], John Preskill[4,9], David R. Reichman[2], Earl T. Campbell[10], Edward F. Valeev[5], Lin Lin[3,11] & Garnet Kin-Lic Chan[1]

No tenemos ventaja cuántica en química...

Abstract

The idea to use quantum mechanical devices to simulate other quantum systems is commonly ascribed to Feynman. Since the original suggestion, concrete proposals have appeared for simulating molecular and materials chemistry through quantum computation, as a potential "killer application" [1, 2, 3, 4, 5]. Indications of potential exponential quantum advantage in artificial tasks [6, 7, 8, 9] have increased interest in this application, thus, it is critical to understand the basis for potential exponential quantum advantage in quantum chemistry. Here we gather the evidence for this case in the most common task in quantum chemistry, namely, ground-state energy estimation. We conclude that evidence for such an exponential advantage across chemical space has yet to be found. While quantum computers may still prove useful for quantum chemistry, it may be prudent to assume exponential speedups are not generically available for this problem.

Simulación de sistemas cuánticos ?

Inicialización: poner el sistema en un estado cuántico dado
Simulación: simular operaciones cuánticas
Lectura del resultado: leer el estado cuántico final

	algoritmo cuántico	algoritmo clásico
Inicialización	exponencial	
Simulación	polinomial	exponencial
Lectura	exponencial	

El reto mayor de la computación cuántica

El reto menor es construir una computadora cuántica (2030?)

- Decenas de compañías compitiendo...
- Tecnologías: fotones, transmons, iones atrapados, átomos fríos, ...
- Objetivo: centenares de qubits lógicos de aquí a 2030

El reto mayor es diseñar algoritmos cuánticos:

1. Con ventaja cuántica
   a. tiempo polinomial
   b. el equivalente clásico es super-polinomial
2. Con valor económico

Porque no tenemos algoritmos cuánticos útiles (hipótesis)

Diseñar algoritmos cuánticos polinomiales es un problema difícil

Poco interés en los algoritmos clásicos superpolinomiales

Los fabricantes de computadoras cuánticas prefieren obviar el problema

Los matemáticos y computistas no han investigado (mucho) el tema

Pesimismo: hay pocos algoritmos con ventaja cuántica (?)