

Prospects of Quantum Computing

Jibran Rashid

August 4, 2025



Quantum Money

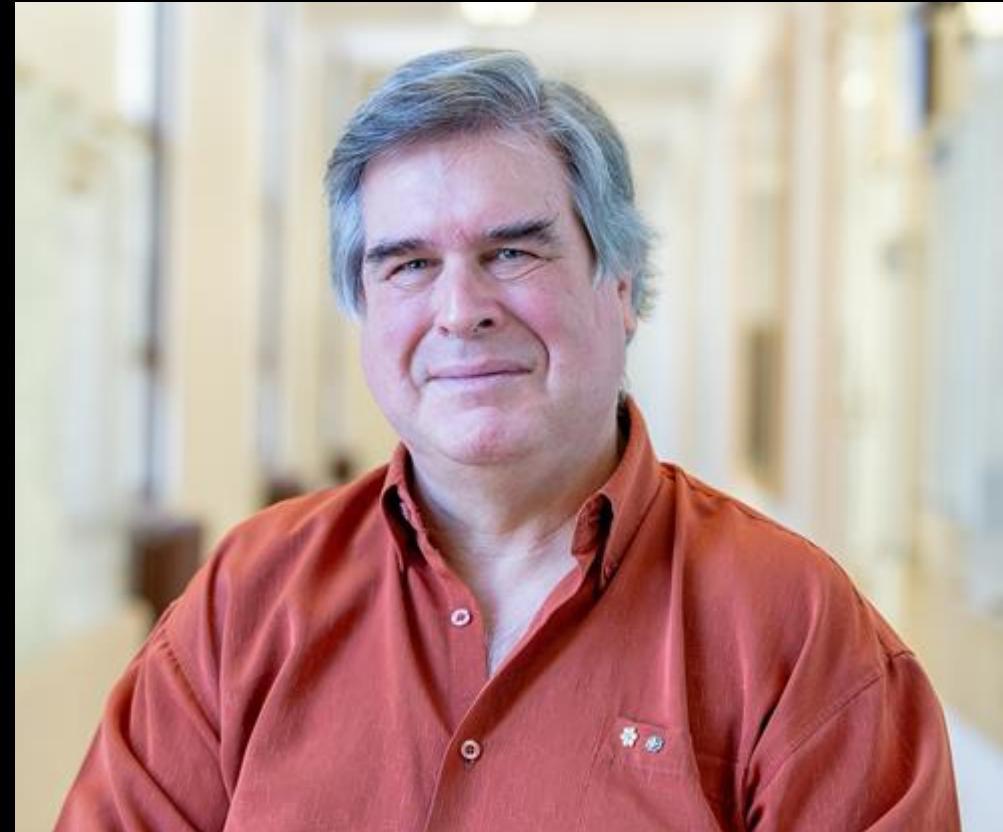


Stephen Wiesner (1942-2021)

Quantum Key Distribution – BB84



Charles Bennett



Gilles Brassard

Simulate Quantum Systems

Now I explicitly go to the question of how we can simulate with a computer

... ***the quantum mechanical effects*** ...

But the full description of quantum mechanics for a large system with R particles is given by a function which we call the amplitude to find the particles at x_1, x_2, \dots, x_R , and therefore because it has too many variables,

it cannot be simulated with a normal computer.



Richard Feynman

Simulate Quantum Systems

Can you do it with a new kind of computer
— **a quantum computer?**

Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements.

It's not a Turing machine, but a machine of a different kind.



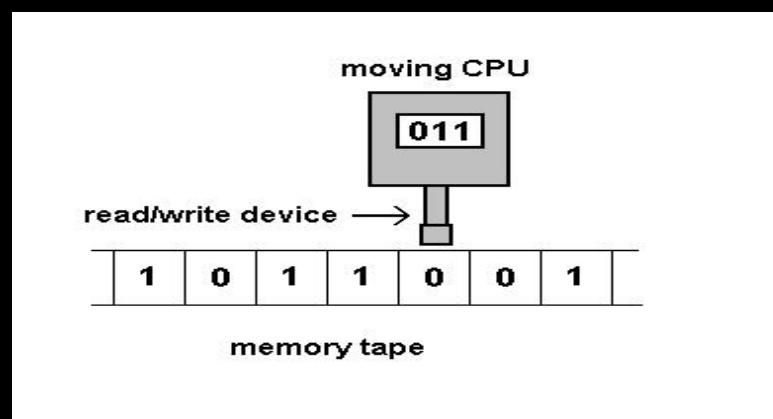
Richard Feynman

The Church-Turing Thesis

“Computable” = Turing-Computable



Alan Turing



Alonzo Church

Fundamental principle linking Computer Science to the real world!

Extended Church-Turing Thesis

Feasibly computable in the physical world

=

Efficiently computable by a Turing machine

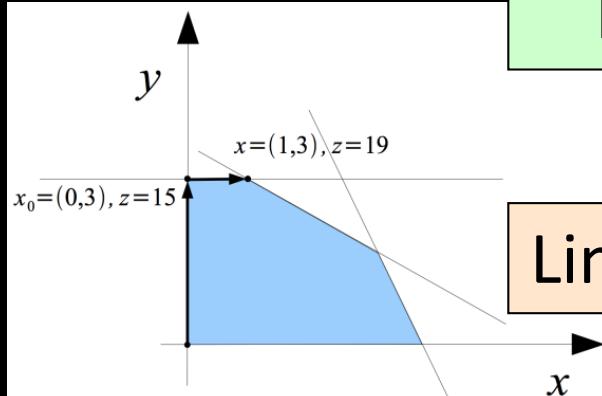
P

Problem: Modeled as a set of binary strings, $L \subseteq \{0,1\}^*$.
Given an **input** $x \in \{0,1\}^*$, the task is to decide if $x \in L$

The class of problems for which there's an algorithm, for a deterministic digital computer, that always correctly decides if $x \in L$, after a number of steps upper-bounded by some polynomial in $|x|$ (the length of x)

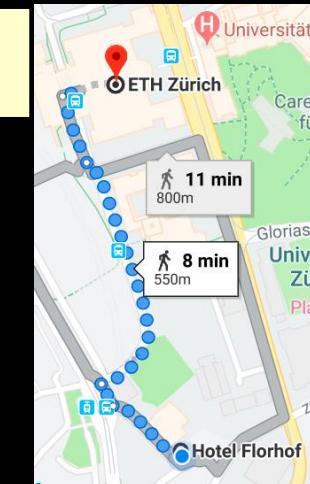
Examples:

Primality
Testing



Connectivity

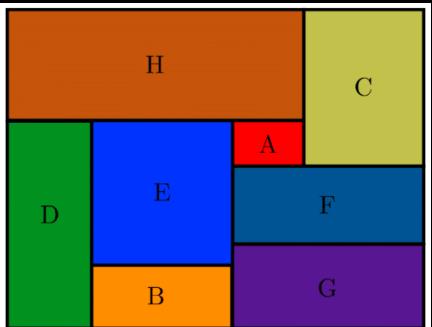
Linear Programming



NP (Nondeterministic Polynomial-Time)

Informally, the class of problems for which there's a polynomial-time algorithm to **recognize** valid solutions (but the solutions might be exponentially hard to **find**)

Examples:

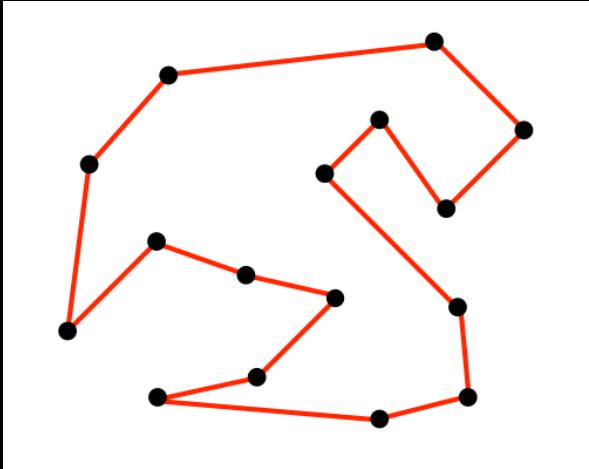


Bin Packing

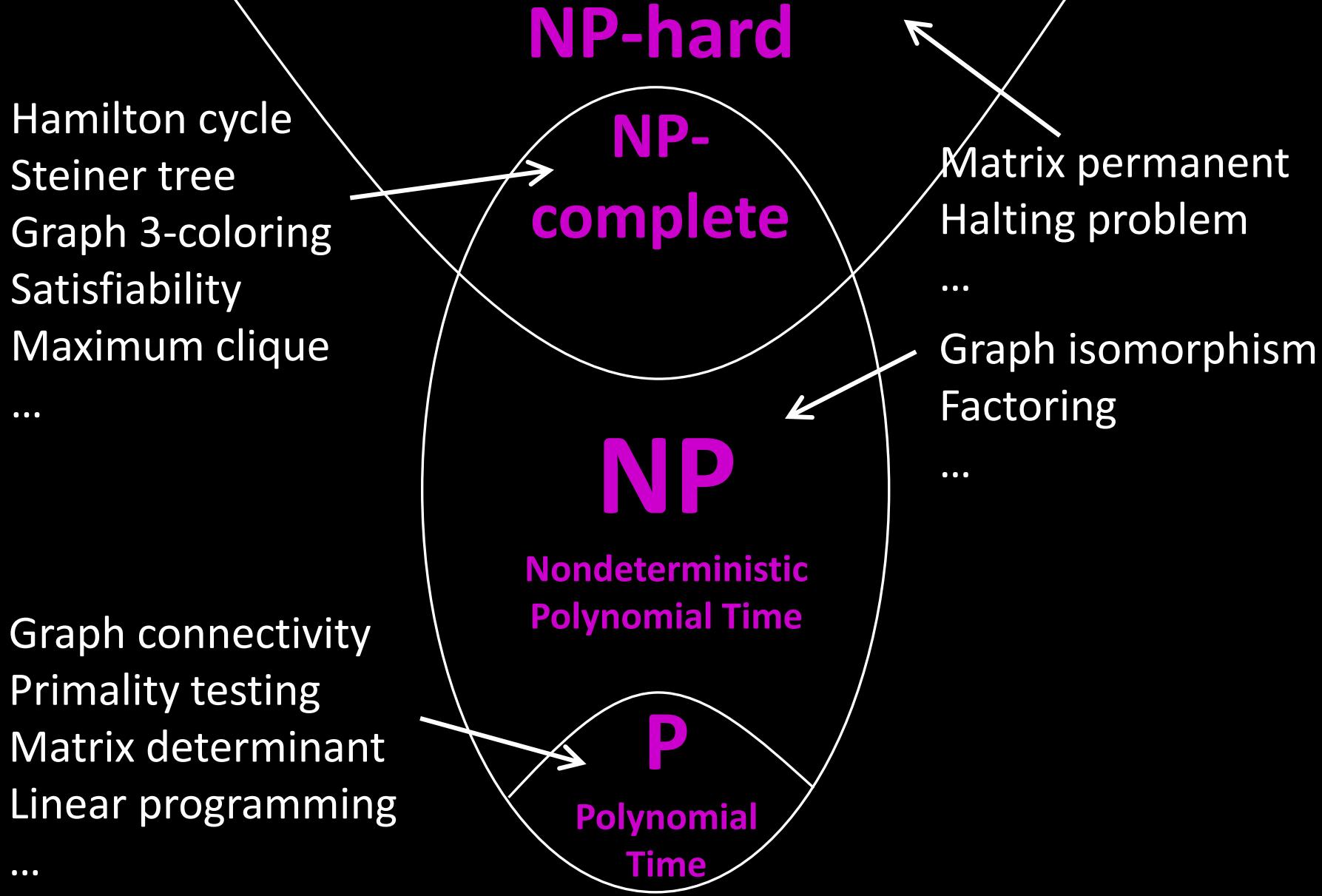
Factoring

Step	Hyp	Ref	Expression
1		efipi 21825	$\bot \vdash (\exp(i \cdot \pi)) = -1$
2	1	oveqlri 6095	$\bot \vdash ((\exp(i \cdot \pi)) + 1) = (-1 + 1)$
3		ax-1cn 9333	$\bot \vdash 1 \in \mathbb{C}$
4		neglcn 10418	$\bot \vdash -1 \in \mathbb{C}$
5		1pnegle0 10423	$\bot \vdash (1 + -1) = 0$
6	3, 4, 5	addcomli 9554	$\bot \vdash (-1 + 1) = 0$
7	2, 6	eqtri 2458	$\bot \vdash ((\exp(i \cdot \pi)) + 1) = 0$

Theorem Proving



Traveling
Salesperson

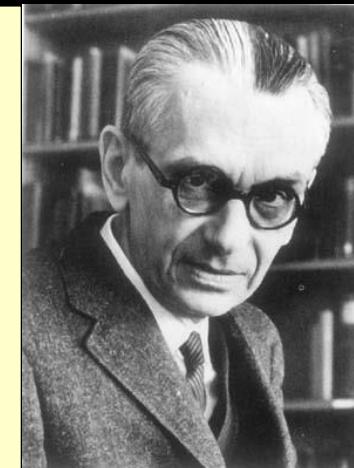


P=N P?

The (literally) \$1,000,000 question

If there actually were a machine with [running time] $\sim Kn$ (or even only with $\sim Kn^2$), this would have consequences of the greatest magnitude.

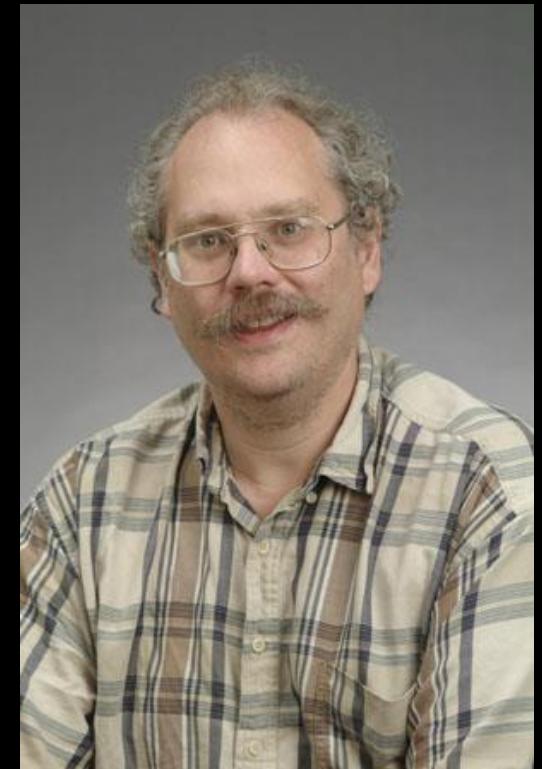
—Gödel to von Neumann, 1956



Integer Factorization is in BQP

Given an integer N, find its prime factors.

Consequently, we can break public-key cryptography systems such as RSA!



Peter Shor

Why Is Building A Quantum Computer So Hard?

Decoherence

**Scalable Quantum Computers
Are Not Possible**

Most re

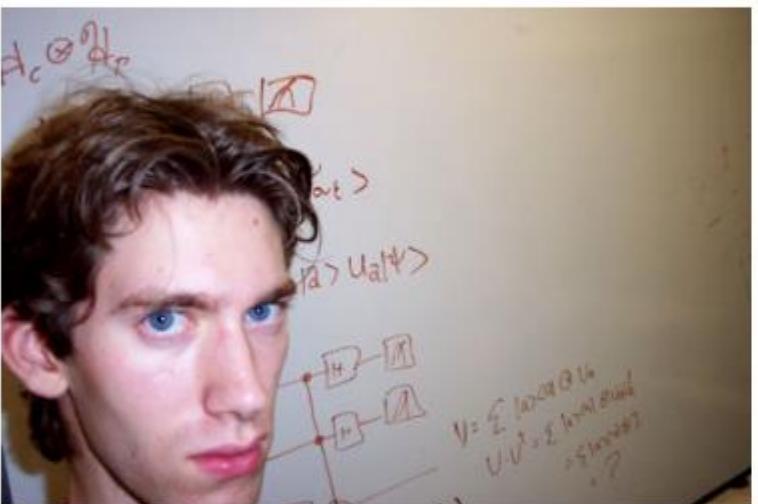
rovides



My Quantum Debate with Aram Harrow: Timeline, Non-technical Highlights, and Flashbacks I

Posted on [March 16, 2013](#) by Gil Kalai

How the debate came about



Gödel's Lost Letter and P=NP

a personal view of the theory of computation

[Home](#) [About P=NP and SAT](#) [About Us](#) [Conventional Wisdom and P=NP](#) [The Gödel Letter](#) [Eak's Paper](#) [Thank You Page](#)

Perpetual Motion of The 21st Century?

JANUARY 30, 2012

by EAKalai

tags: QIP, Machine, quantum

SUBSCRIBE TO GÖDEL'S LOST LETTER



View and press enter

RECENT POSTS

- [Gödel's Theorem: The Movie](#)
- [The Crows Game Affair](#)
- [Back To The Past](#)
- [Predictions and Principles](#)
- [The Year That Was](#)



(Email from Aram Harrow, June 4, 2011) Dear Gil Kalai, I am a quantum computing researcher, and was wondering about a few points in [your paper](#)...

(Aram's email was detailed and thoughtful and at the end he proposed to continue the discussion privately or as part of a public discussion.)

A Win-Win Situation

Scalable Quantum Computers Are Possible

Quantum Simulation

Quantum Chemistry

Factorization

Optimization and Machine Learning

...

A Win-Win Situation

Scalable Quantum Computers Are Not Possible

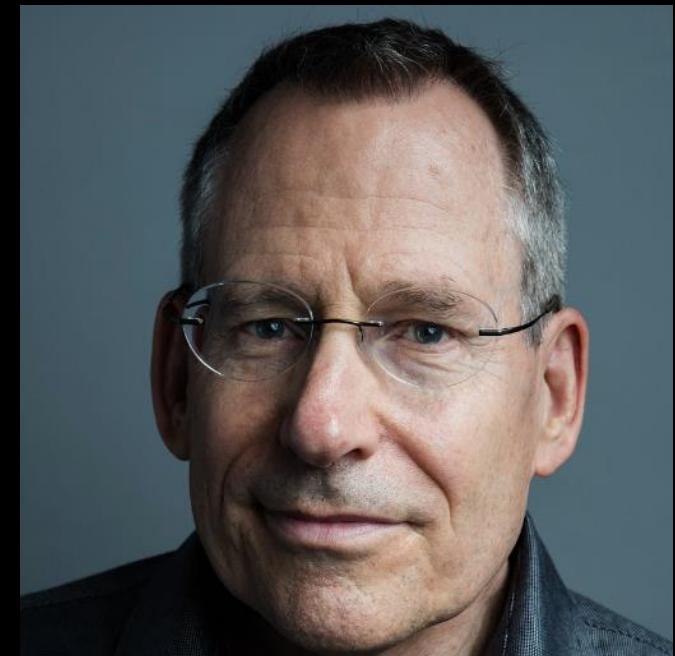
A Win-Win Situation

**Scalable Quantum Computers Are Not Possible
New Physics!**

NISQ Era

Noisy Intermediate-Scale Quantum: ... size of quantum computers which will be available in the next few years, with a number of qubits ranging from **50** to a few hundred.

“Noisy” emphasizes that we’ll have imperfect control over those qubits; the noise will place serious limitations on what quantum devices can achieve in the near term.



John Preskill

Quantum Computational Advantage

Use of a quantum computer to solve **some** well-defined problem
much faster than **any** available classical computer running **any**
known algorithm

Quantum technologies

+ Add to myFT

Google claims to have reached quantum supremacy

Google may have just ushered in an era of 'quantum supremacy'

'The first computation that can only be performed on a quantum processor'

By Jon Porter | @JonPorty | Sep 23, 2019, 7:06am EDT

f t SHARE



Google's 'Quantum Supremacy' Isn't the End of Encryption

Google said its quantum computer outperformed conventional models. But it will take time for anything practical.



MOTHERBOARD
TECH BY VICE

OK, WTF Is Google's 'Quantum Supremacy'?

Google has reached quantum supremacy – here's what it should do next



TECHNOLOGY | ANALYSIS 26 September 2019

By Chelsea Whyte



NEWS

QUANTUM PHYSICS

Rumors hint that Google has accomplished quantum supremacy

Reports suggest a quantum computer has surpassed standard computers on a specific type of calculation

Google claims to have reached quantum supremacy

IBM's Response

Using Summit, the largest supercomputer currently on earth—which fills 2 basketball courts and has 250 petabytes of hard disk—it should be possible to simulate Google's 3-minute calculation in ~2.5 days, rather than the 10,000 years Google estimated



supremacy

Reports suggest a quantum computer has surpassed standard computers on a specific type of calculation

SCIENTIFIC
AMERICAN®

QUANTUM COMPUTING

Light-Based Quantum Computer Exceeds Fastest Classical Supercomputers

The setup of lasers and mirrors effectively “solved” a problem far too complicated for even the largest traditional computer system

Light-Based Quantum Computer Exceeds Fastest Classical Supercomputers

The setup can achieve **Quantum supremacy, now with BosonSampling**—the ability to perform calculations that would take even the fastest classical supercomputer exponentially longer.

A group led by Jianwei Pan and Chao-Yang Lu, based mainly at USTC in Hefei, China, announced today that it achieved BosonSampling with 40–70 detected photons—up to and beyond the limit where a classical supercomputer could feasibly verify the results. (Technically, they achieved a variant called Gaussian

Quantum Manifesto

A New Era of Technology

May 2016



This manifesto is a call to launch an ambitious European initiative in quantum technologies, needed to ensure Europe's leading role in a technological revolution now under way.



President Trump has signed a \$1.2 billion law to boost US quantum tech

The new National Quantum Initiative Act will give America a national master plan for advancing quantum technologies.

This manifesto is a call to launch an ambitious European initiative in quantum technologies, needed to ensure Europe's leading role in a technological revolution now under way.

SCIENTIFIC
AMERICAN®

QUANTUM COMPUTING

China Is Pulling Ahead in Global Quantum Race, New Studies Suggest

The competition between the U.S. and China over development of quantum technology has implications for both the future of science and the two countries' political relations

now under way.

China] P The adv

The competition bet
implications for

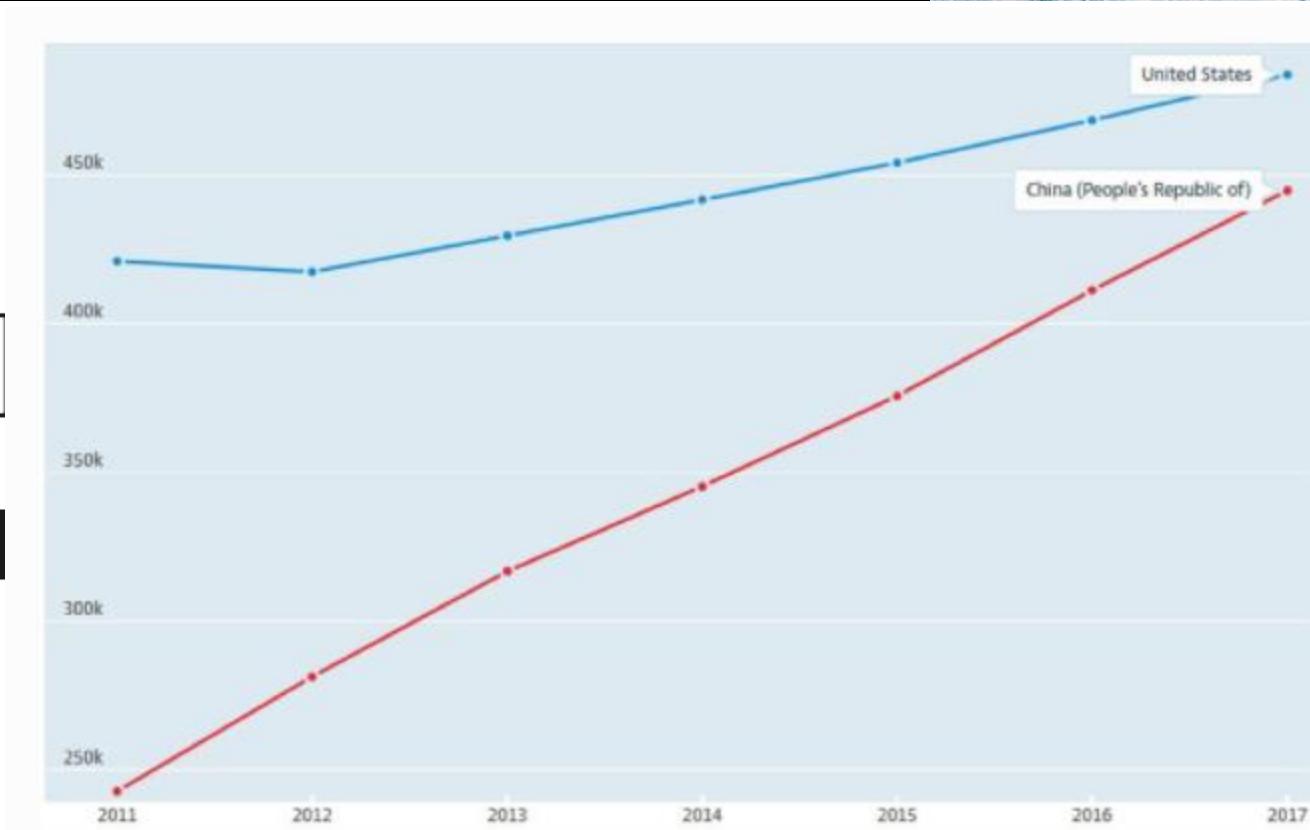
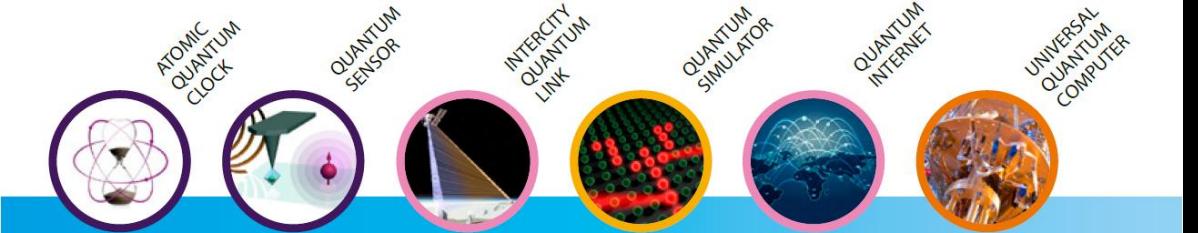


Figure 1: USA vs. China total annual R&D expenditure (millions of dollars) OECD
SCIENCE, TECHNOLOGY & R&D STATISTICS

Global Studies

Quantum technology has
political relations
now under way.



2015 → 2035



0 – 5 years

- A Core technology of quantum repeaters
- B Secure point-to-point quantum links

5 – 10 years

- C Quantum networks between distant cities
- D Quantum credit cards

> 10 years

- E Quantum repeaters with cryptography and eavesdropping detection
- F Secure Europe-wide internet merging quantum and classical communication

- A Simulator of motion of electrons in materials
- B New algorithms for quantum simulators and networks

- C More precise atomic clocks for synchronisation of future smart networks, incl. energy grids

- C Development and design of new complex materials
- D Versatile simulator of quantum magnetism and electricity

- C Quantum sensors for larger volume applications including automotive, construction
- D Handheld quantum navigation devices

- E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design

- E Gravity imaging devices based on gravity sensors
- F Integrate quantum sensors with consumer applications including mobile devices

- A Operation of a logical qubit protected by error correction or topologically

- B New algorithms for quantum computers

- C Small quantum processor executing technologically relevant algorithms

- D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit

- E Integration of quantum circuit and cryogenic classical control hardware

- F General purpose quantum computers exceed computational power of classical computers

Potential Applications of Quantum Computers

- **Probably**

- Cryptography
- Optimization
- Simulation
- Science
- Philosophy

Potential Applications of Quantum Computers

- **Probably**
 - Cryptography
 - Optimization
 - Simulation
 - Science
 - Philosophy
- **Maybe**
 - Machine Learning
 - Dequantization

Potential Applications of Quantum Computers

- **Probably:**

- Cryptography
- Optimization
- Simulation
- Science
- Philosophy

- **Maybe**

- Machine Learning
- Dequantization

- **Not Really:**

- Efficiently solve NP-Complete problems

Potential Applications of Quantum Computers

- **Probably**

- Cryptography
- Optimization
- Simulation
- Science
- Philosophy

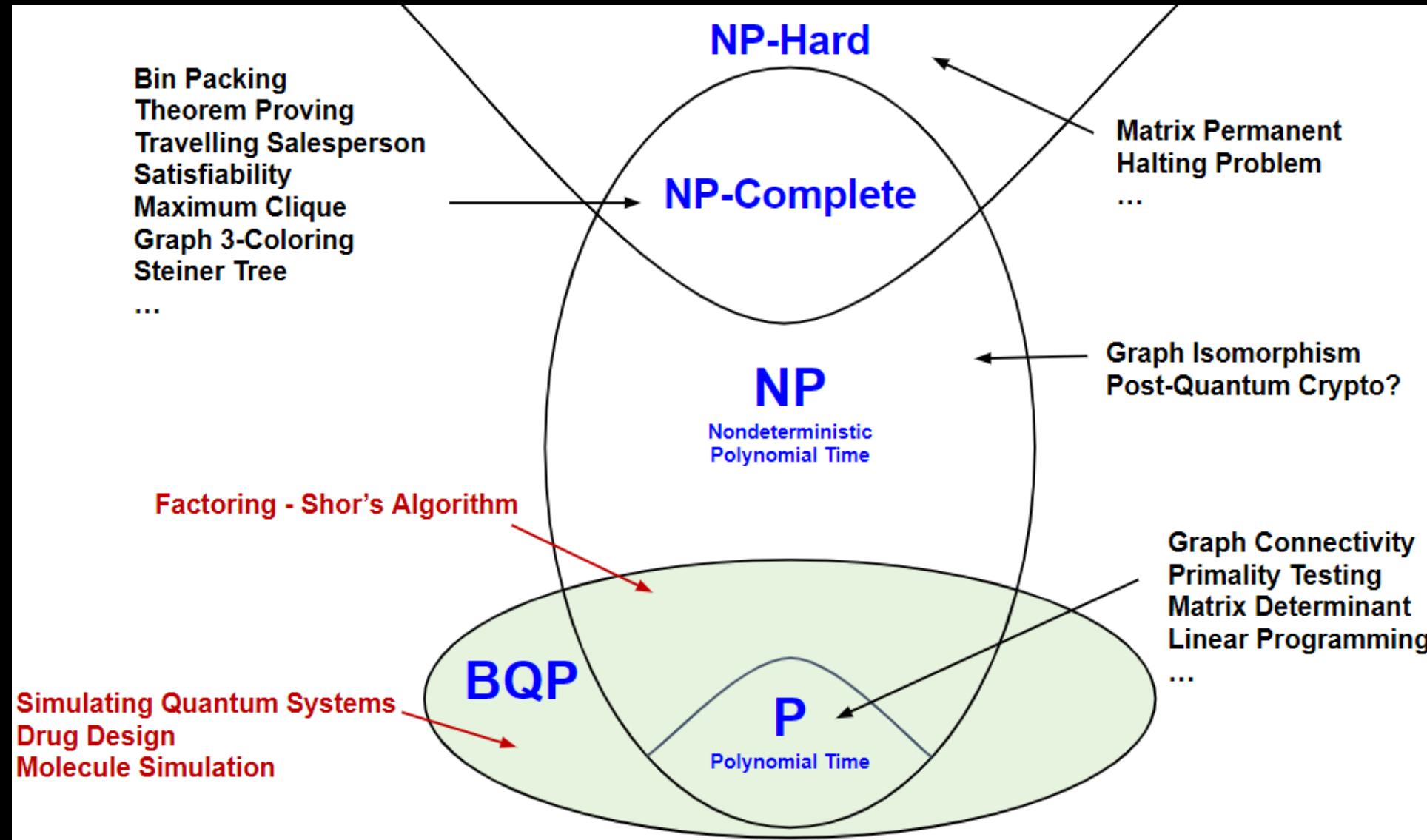
- **Maybe**

- Machine Learning
 - Dequantization
- *Contribute towards ending world hunger, ending climate change, finding aliens...*

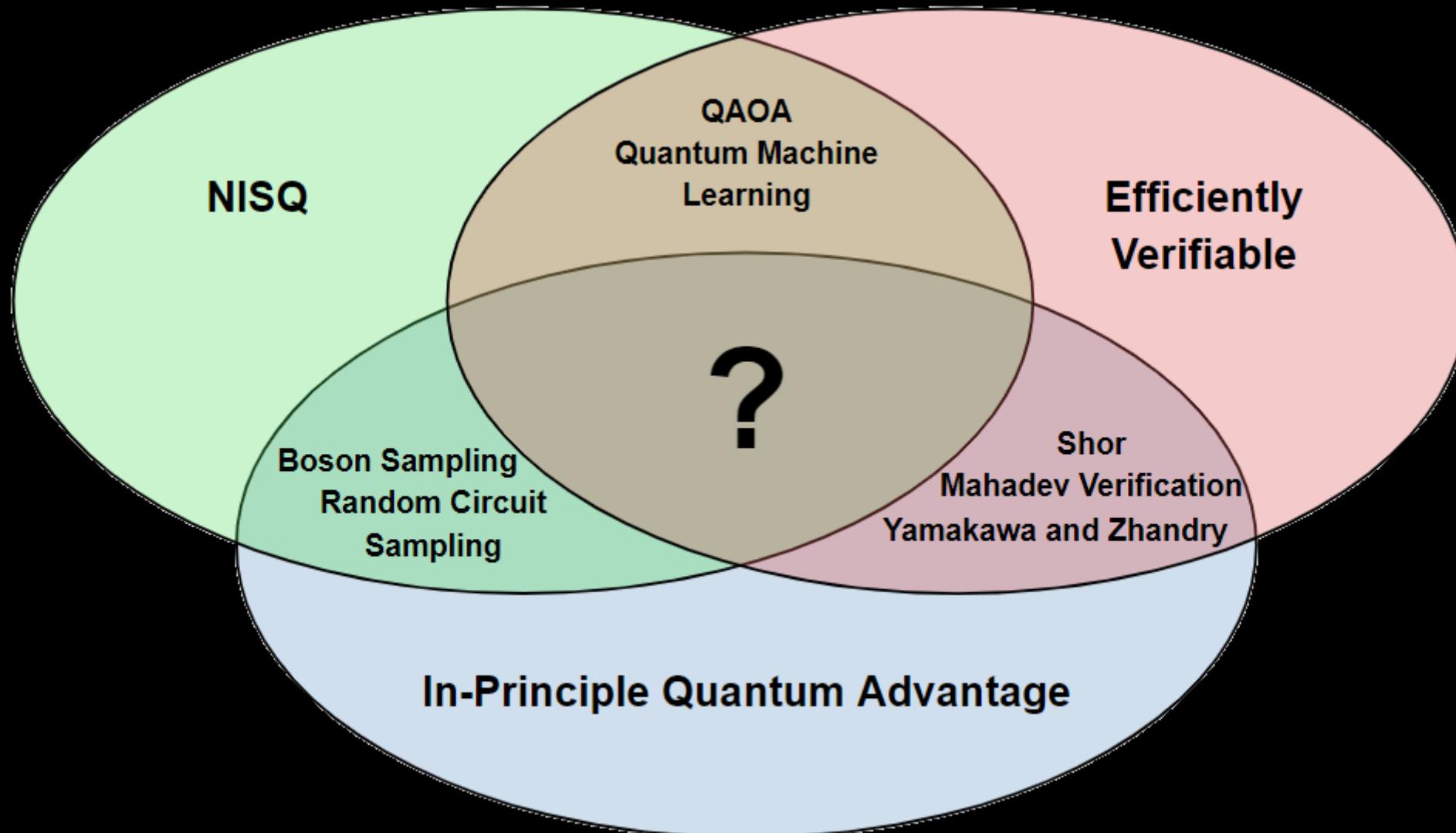
- **Not Really:**

- Efficiently solve NP-Complete problems

What Problems do we Expect QC to Solve?



What Problems do we Expect QC to Solve?



Challenges

- Quantum Compiler Design
- Benchmarking Quantum Software
- Error Mitigation Versus Error Correction
- New Ideas...

Challenges

- Quantum Compiler Design
- Benchmarking Quantum Software
- Error Mitigation Versus Error Correction
- New Ideas...

Need Interdisciplinary Education Initiatives!

Thank You!