Introduction to Quantum Computing

Jibran Rashid

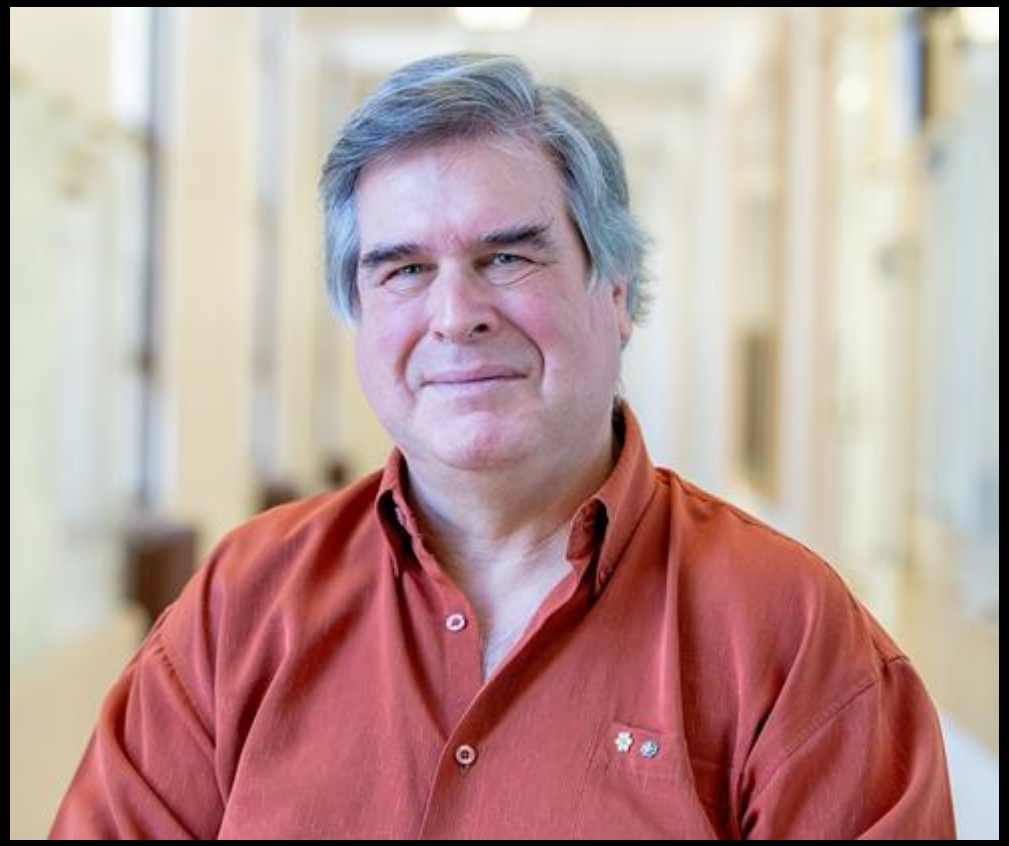
February 17, 2025

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 x1, x2, . . . xR, 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,

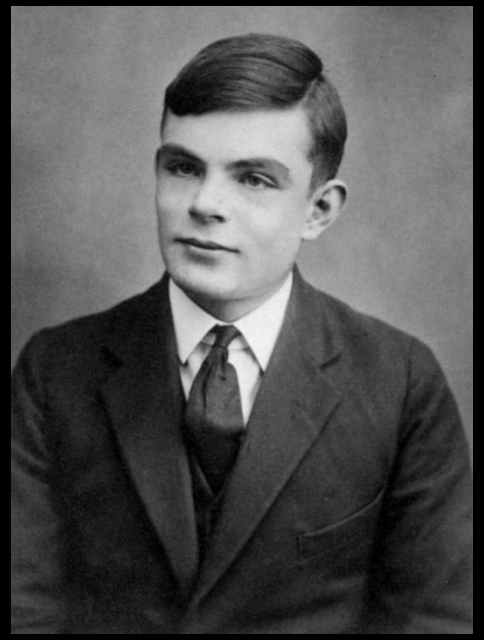
with quantum computer elements.

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

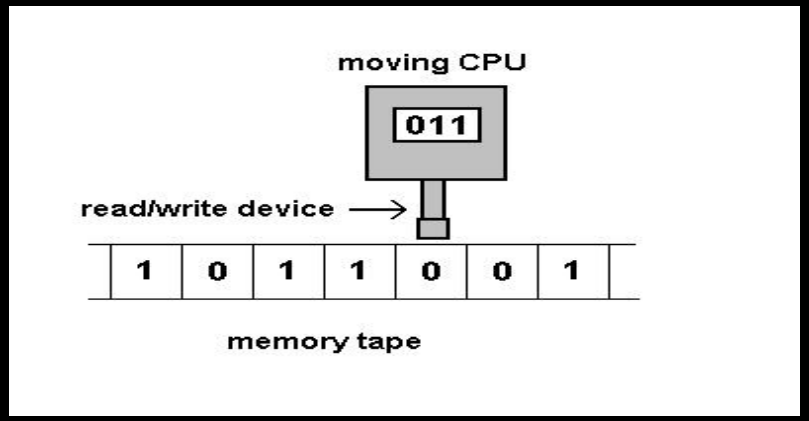
Richard Feynman

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

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 $x \in L$

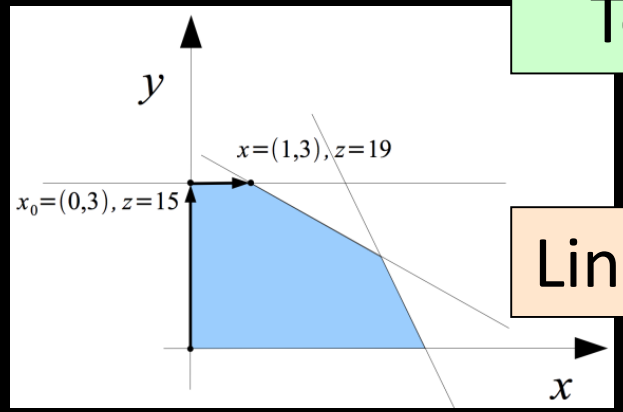
P

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)

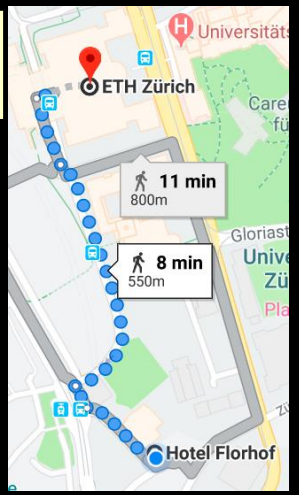
Examples:

Primality Testing

Connectivity



Linear Programming

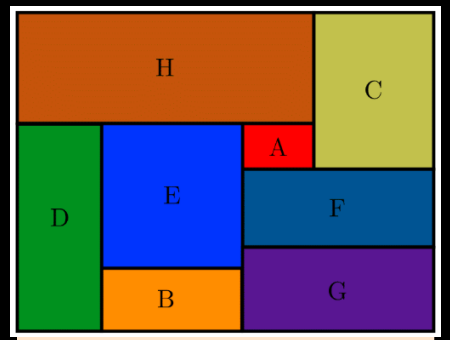


NP (Nondeterministic Polynomial-Time)

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:

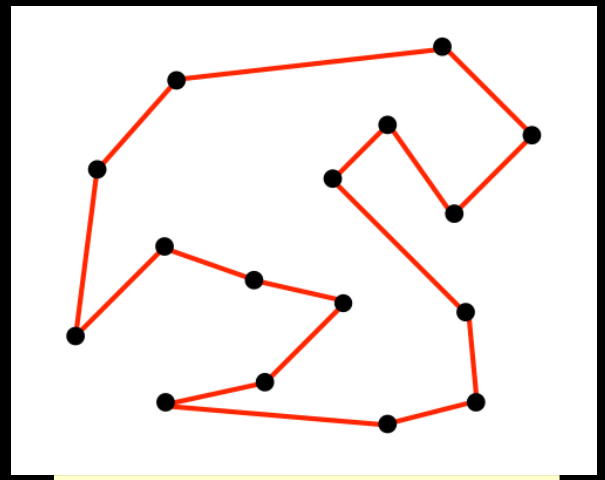
Factoring



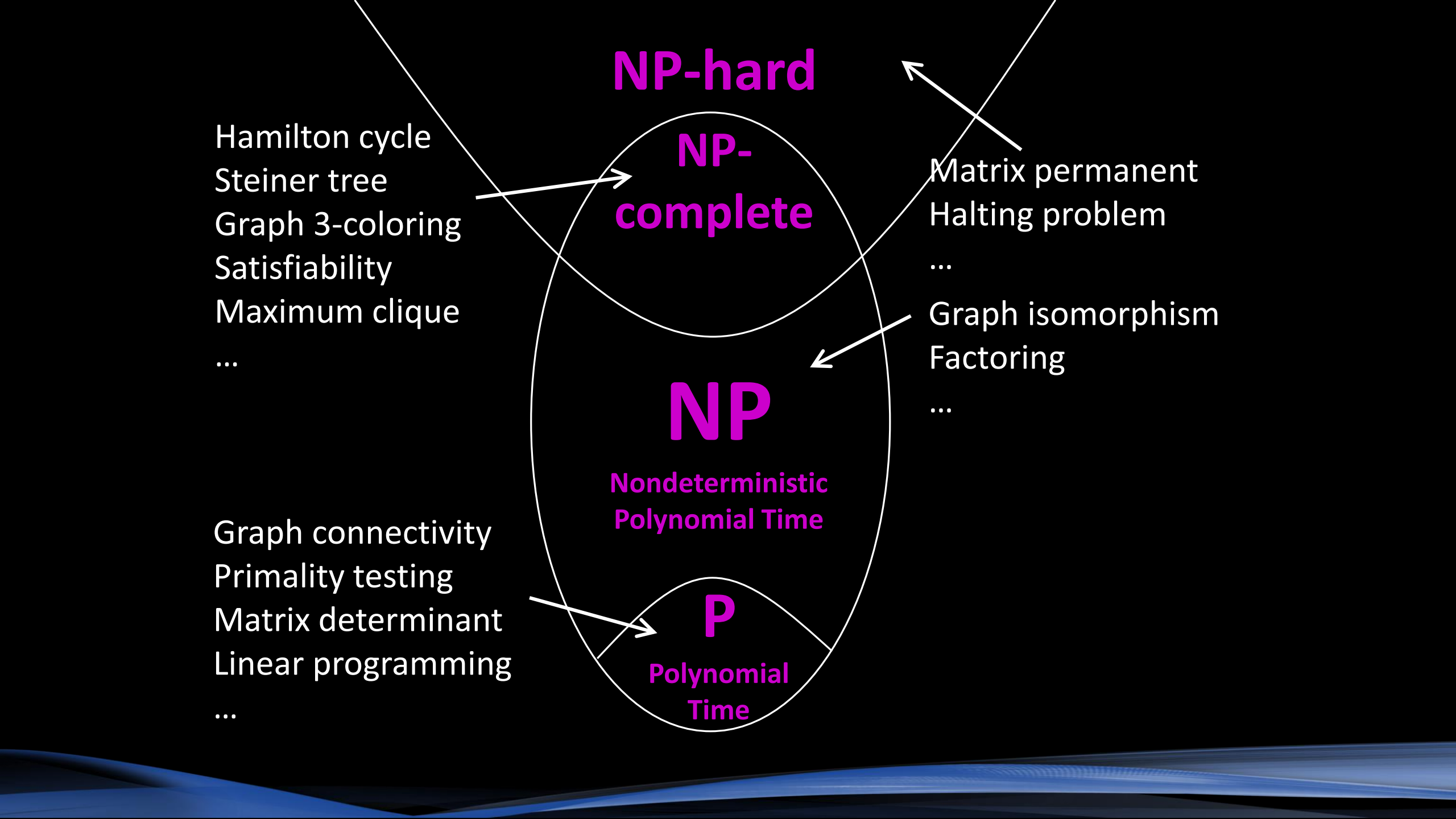
Bin Packing

Step	Hyp	Ref	Expression
1		efipi 21825	$\vdash (\exp(i \cdot \pi)) = -1$
2	1	oveq1i 6095	$\vdash ((\exp(i \cdot \pi)) + 1) = (-1 + 1)$
3		ax-1cn 9333	$\vdash 1 \in \mathbb{C}$
4		neg1cn 10418	$\vdash -1 \in \mathbb{C}$
5		1pneg1e0 10423	$\vdash (1 + -1) = 0$
6	3, 4, 5	addcomli 9554	$\vdash (-1 + 1) = 0$
7	2, 6	eqtri 2458	$\vdash ((\exp(i \cdot \pi)) + 1) = 0$

Theorem Proving



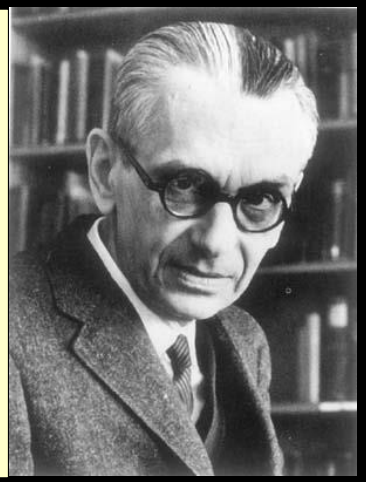
Traveling Salesperson


NP-hard
NP-complete
NP
Nondeterministic Polynomial Time
P
Polynomial Time
Hamilton cycle
Steiner tree
Graph 3-coloring
Satisfiability
Maximum clique
…
Matrix permanent
Halting problem
…
Graph isomorphism
Factoring
…
Graph connectivity
Primality testing
Matrix determinant
Linear programming
…

P=NP?

The (literally) $1,000,000 question

If there actually were a machine with [running time] ~Kn (or even only with ~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

Most re **rovides**

Scalable Quantum Computers
Are Not Possible

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

(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

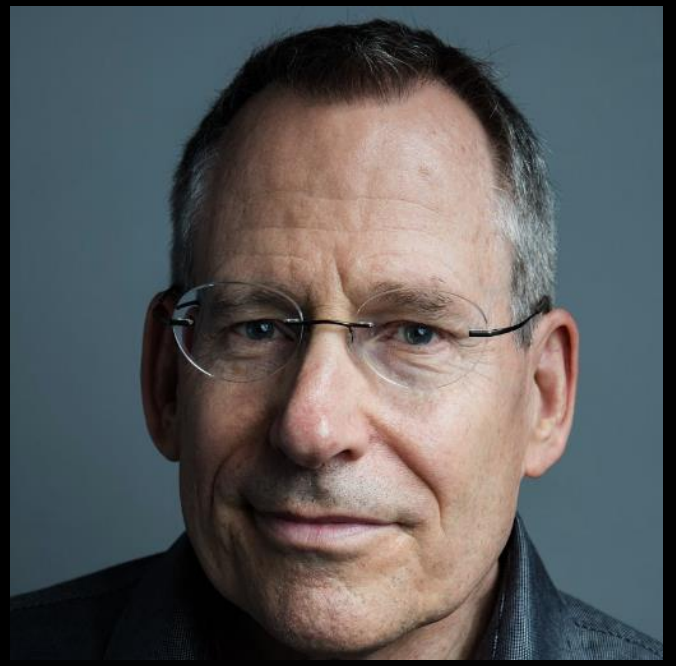
Scalable Quantum Computers Are Not Possible

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

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

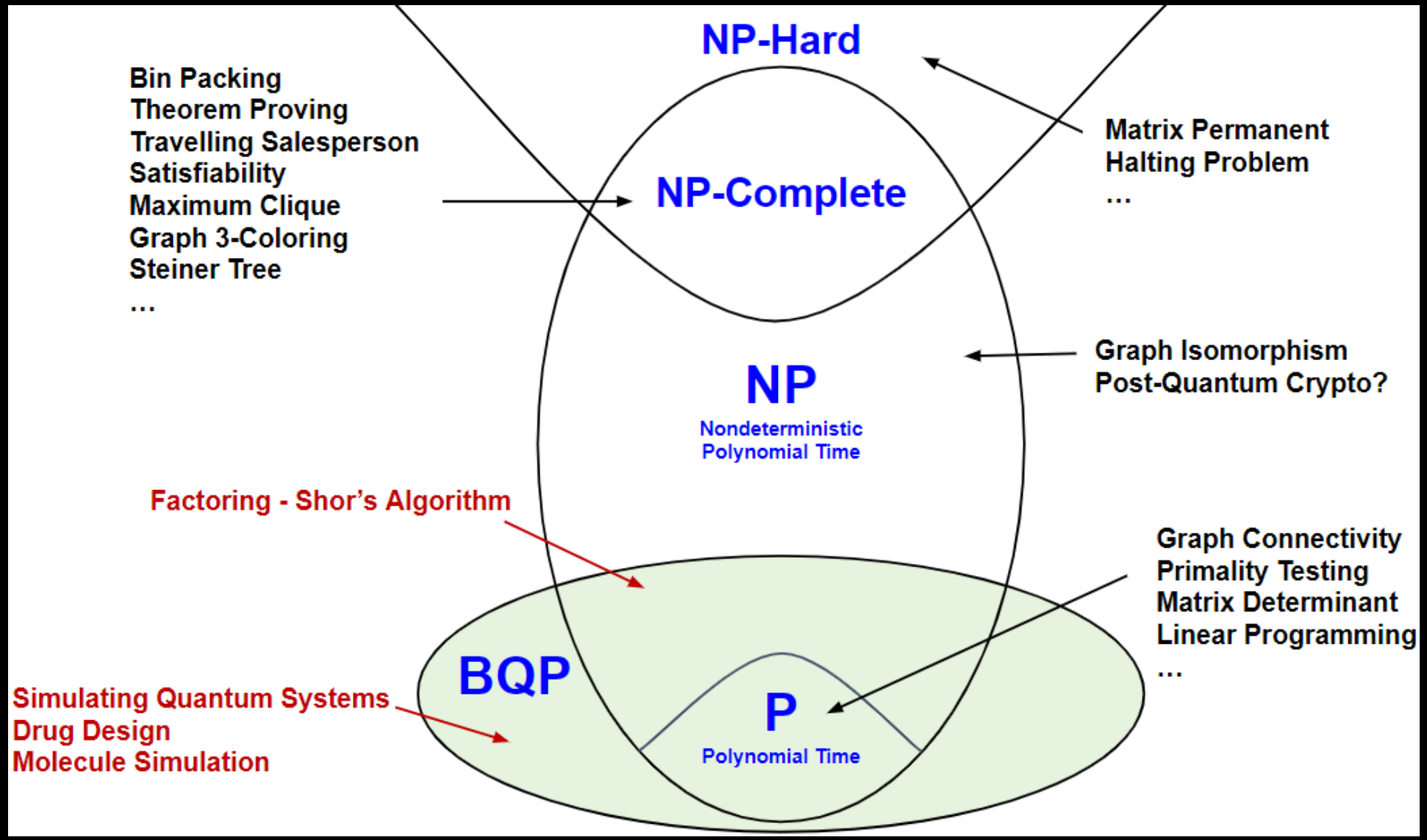
Potential Applications of Quantum Computers

- **Probably**
  - Cryptography
  - Optimization
  - Simulation
  - Science
  - Philosophy
- **Maybe**
  - Machine Learning
    - Dequantization
- **Not Really:**
  - Efficiently solve NP-Complete problems

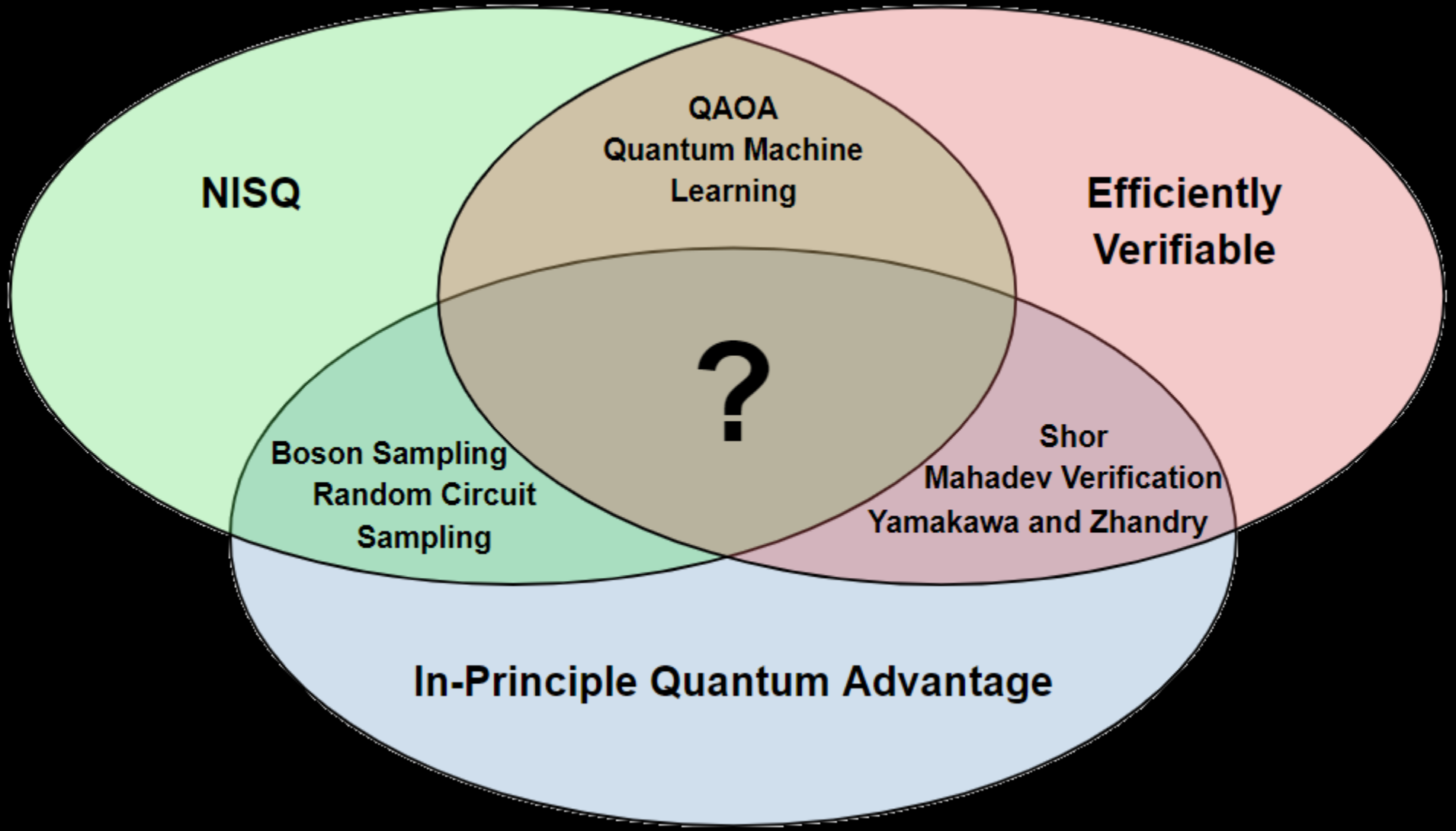
Potential Applications of Quantum Computers

- **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…

Thank You!