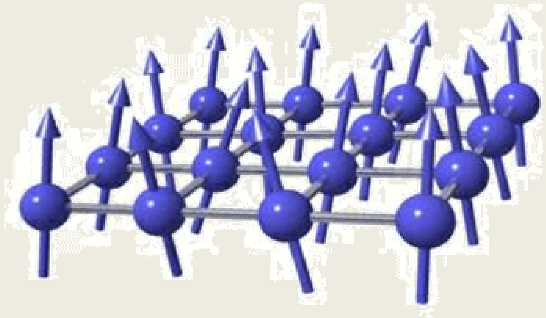
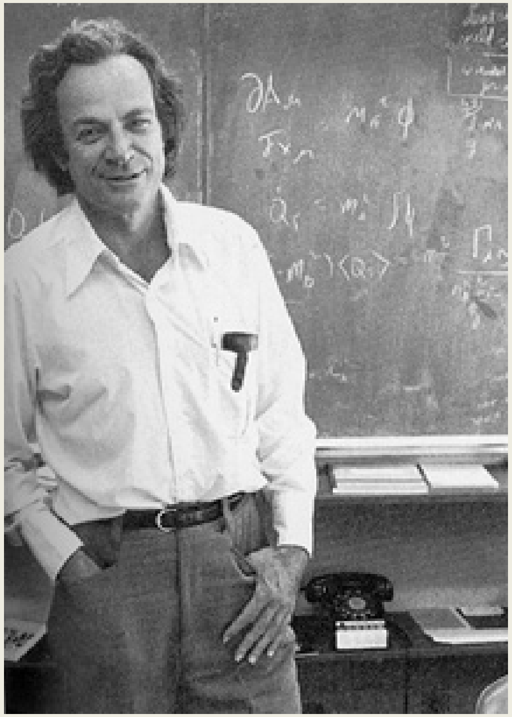


An Introduction to Quantum Computation

Sandy Irani
Department of Computer Science
University of California, Irvine

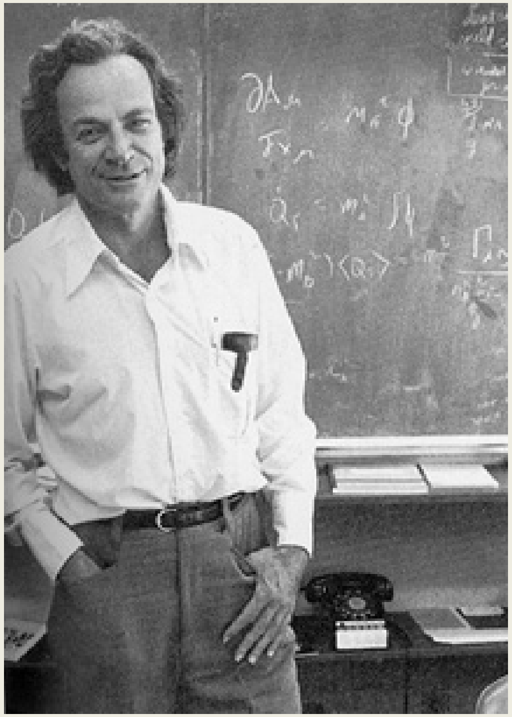
- "Simulating Physics with Computers"

  Richard Feynman – Keynote Talk, 1st Conference on Physics and Computation, MIT, 1981



- “Simulating Physics with Computers”

  Richard Feynman – Keynote Talk, 1st Conference on Physics and Computation, MIT, 1981



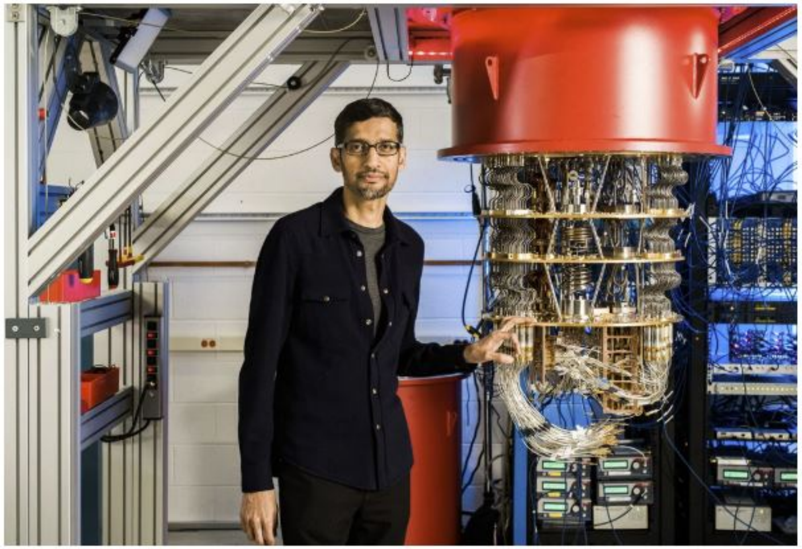
Is it possible to build computers that use the laws of quantum mechanics to compute?

ENGLISH ESPAÑOL 中文

The New York Times

The Week in Tech: Google's Quantum Leap

The company can run esoteric calculations on exotic new hardware faster than is possible on a supercomputer. It's an achievement of little practical use, but still important.



Google's chief executive of Google, Sundar Pichai, with its quantum computer. Google

By Jamie Condliffe and Nicole Perlroth

Oct. 25, 2019

Church-Turing Thesis

"Until recently, every computer on the planet – from a 1960's mainframe to your iPhone…- has operated by the same set of rules. These were the rules that Charles Babbage understood in the 1830's and that Alan Turing codified in the 1930's. Through the course of the computer revolution, all that has changed at the lowest level are the numbers: speed, amount of RAM and hard disk, number of parallel processors."

"But quantum computing is different."

--Scott Aaronson

NY Times Oct 30, 2019

What’s so special about a Quantum Computer?

Quantum Superposition

$\frac{1}{\sqrt{2}}\Big|$  $\Big\rangle + \frac{1}{\sqrt{2}}\Big|$  $\Big\rangle$

Quantum Superposition

$-\frac{1}{\sqrt{2}}\Big|$  $\Big\rangle - \frac{1}{\sqrt{2}}\Big|$  $\Big\rangle$

Quantum Superposition

Implementations of a "Qubit"

- Energy level of an atom
- Spin orientation of an electron
- Polarization of a photon.
- NMR, Ion traps,...

Information: 1 Bit Example (Schrodinger's Cat)

- Classical Information:
  - A bit is in state 0 or state 1

X=1

OR

X=0

- Classical Information with Uncertainty
  - Bit is 0 with probability p_0
  - Bit is 1 with probability p_1
  - State (p_0, p_1)

- Quantum Information
  - State is a *superposition* over states 0 and 1
  - State is (α_0, α_1) where α_0, α_1 are **complex**.

Information: 1 Bit Example (Schrodinger's Cat)

- Classical Information:
  - A bit is in state 0 or state 1
- Classical Information with Uncertainty
  - Bit is 0 with probability p_0
  - Bit is 1 with probability p_1
  - State (p_0, p_1)
- Quantum Information
  - State is a *superposition* over states 0 and 1
  - State is (α_0, α_1) where α_0, α_1 are **complex**.

X=1

OR

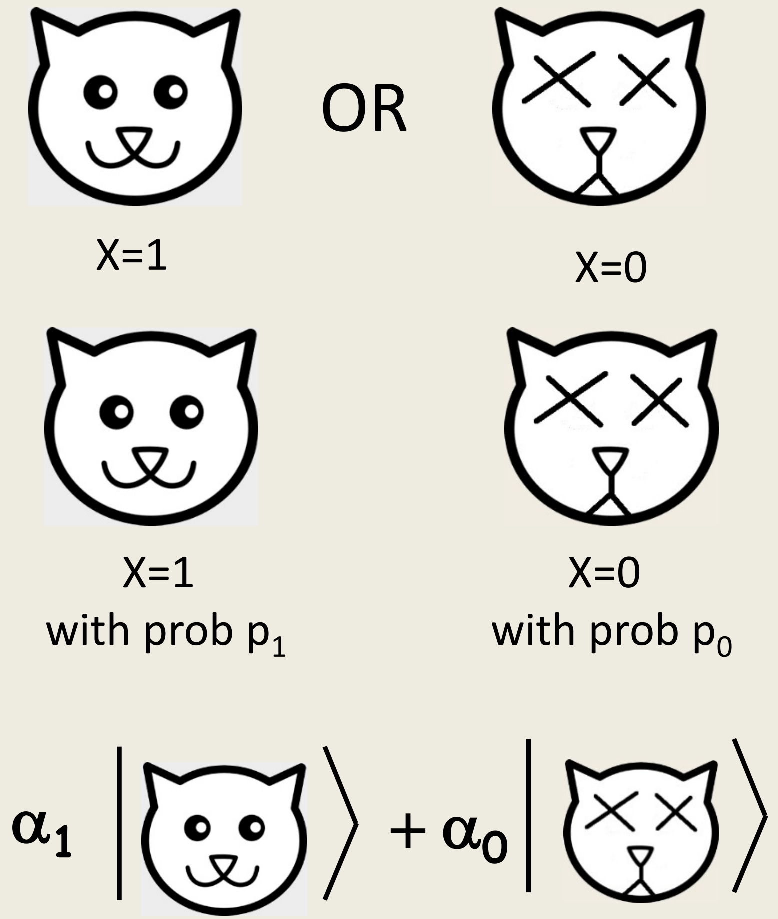
X=0

X=1 with prob p_1

X=0 with prob p_0

Information: 1 Bit Example (Schrodinger's Cat)

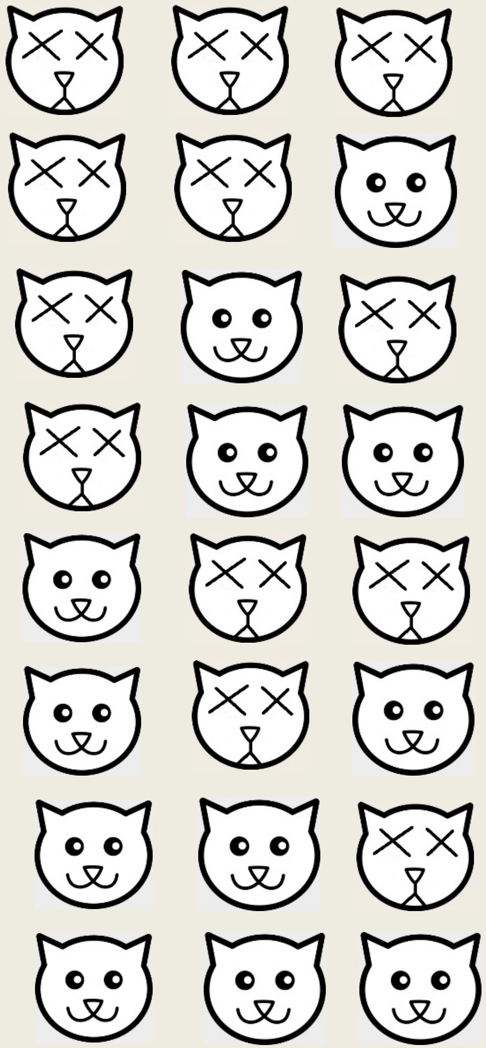
- Classical Information:
  - A bit is in state 0 or state 1
- Classical Information with Uncertainty
  - State (p_0, p_1)
- Quantum Information
  - State is partly 0 and partly 1
  - State is (α_0, α_1) where α_0, α_1 are **complex**.



Information: n Bit Example

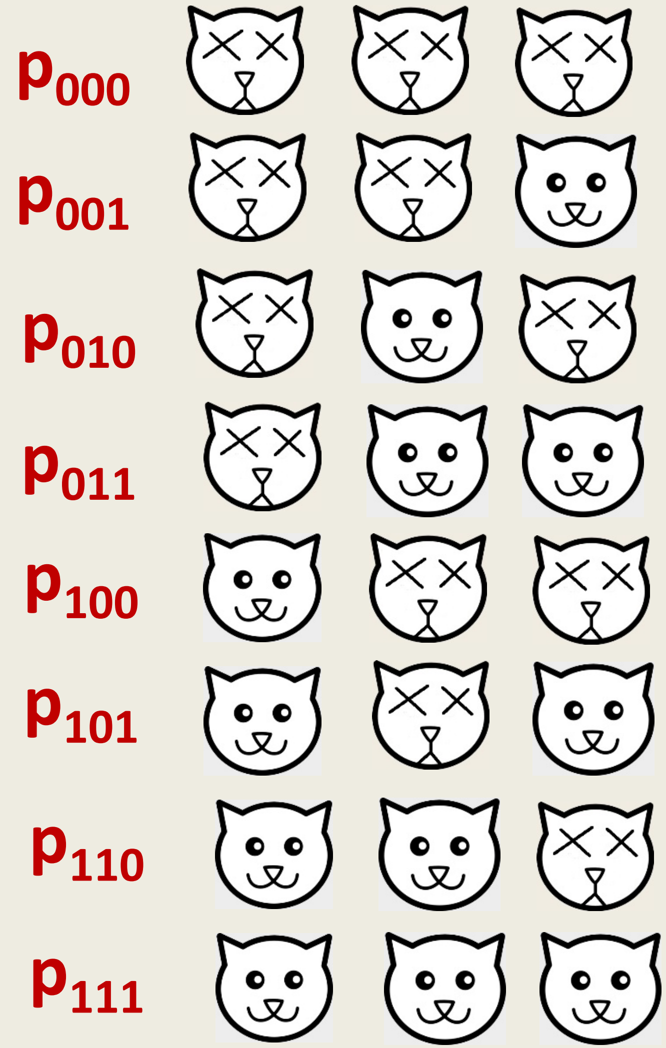
- Classical Information:
  - State of n bits specified by a string x in $\{0,1\}^n$
- Classical Information with Uncertainty
  - State described by probability distribution over 2^n possibilities
  - $(p_0, p_1, \ldots, p_{2^n-1})$
- Quantum Information
  - State is a superposition over 2^n possibilities
  - $(\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1})$, where a is complex

X = 011



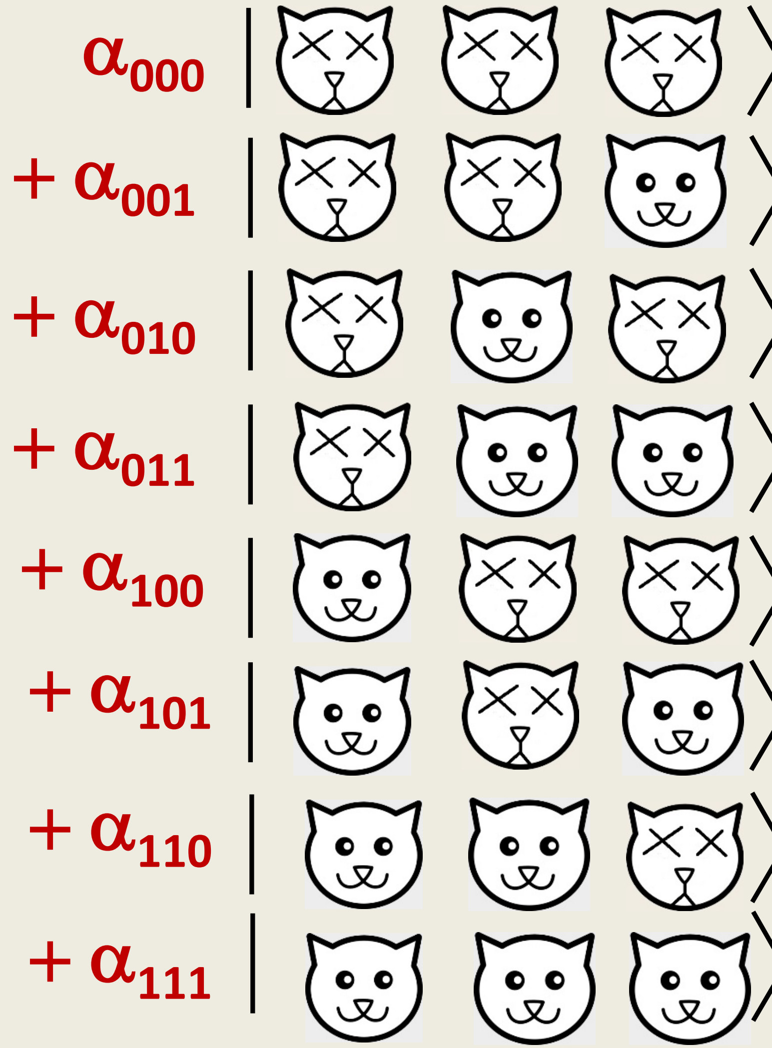
Information: n Bit Example

- Classical Information:
  - State of n bits specified by a string x in $\{0,1\}^n$
- Classical Information with Uncertainty
  - State described by probability distribution over 2^n possibilities
  - $(p_0, p_1, \ldots, p_{2^n-1})$
- Quantum Information
  - State is a superposition over 2^n possibilities
  - $(\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1})$, where a is complex



Information: n Bit Example

- Classical Information:
  - State of n bits specified by a string x in $\{0,1\}^n$
- Classical Information with Uncertainty
  - State described by probability distribution over 2^n possibilities
  - $(p_0, p_1, \ldots, p_{2^n-1})$
- Quantum Information
  - State is a superposition over 2^n possibilities
  - $(\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1})$, where a is complex



- A quantum kilobyte of data

  (8192 qubits)

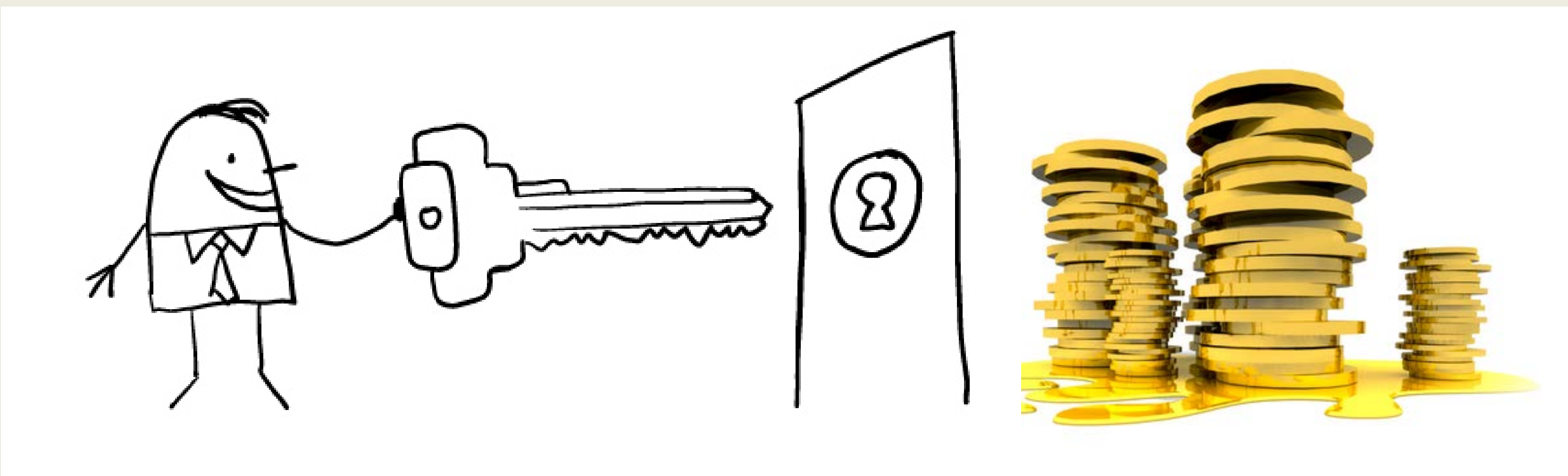
  Encodes 2^{8192} complex numbers

  $2^{8192} \sim 10^{2466}$

  (Number of atoms in the universe $\sim 10^{82}$)

- State of n qubits $(\alpha_0,\ldots,\alpha_{2^n-1})$ stores 2^n complex numbers:

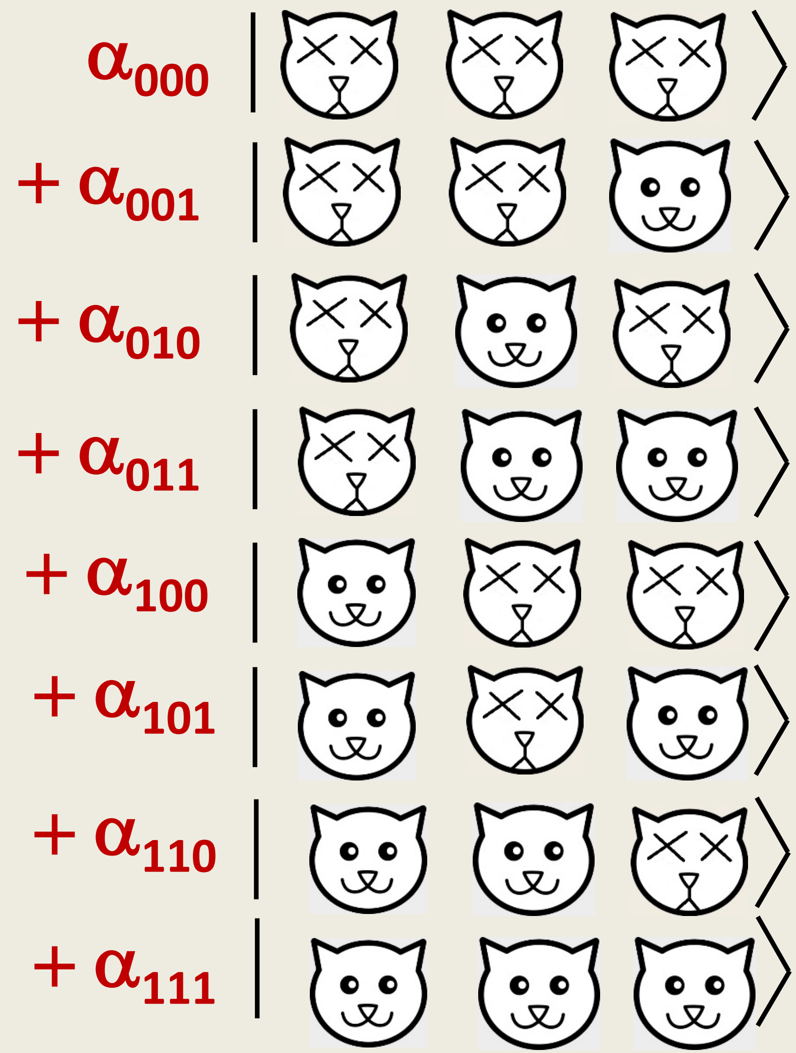
Rich in information



How to use it?
How to access it?

Quantum Measurement

- State of n qubits $(\alpha_0,\ldots,\alpha_{2^n-1})$
- If all n qubits are examined:
  - Outcome is
    010 with probability $|\alpha_{010}|^2$.



Quantum Measurement

- State of n qubits $(\alpha_0,\ldots,\alpha_{2^n-1})$

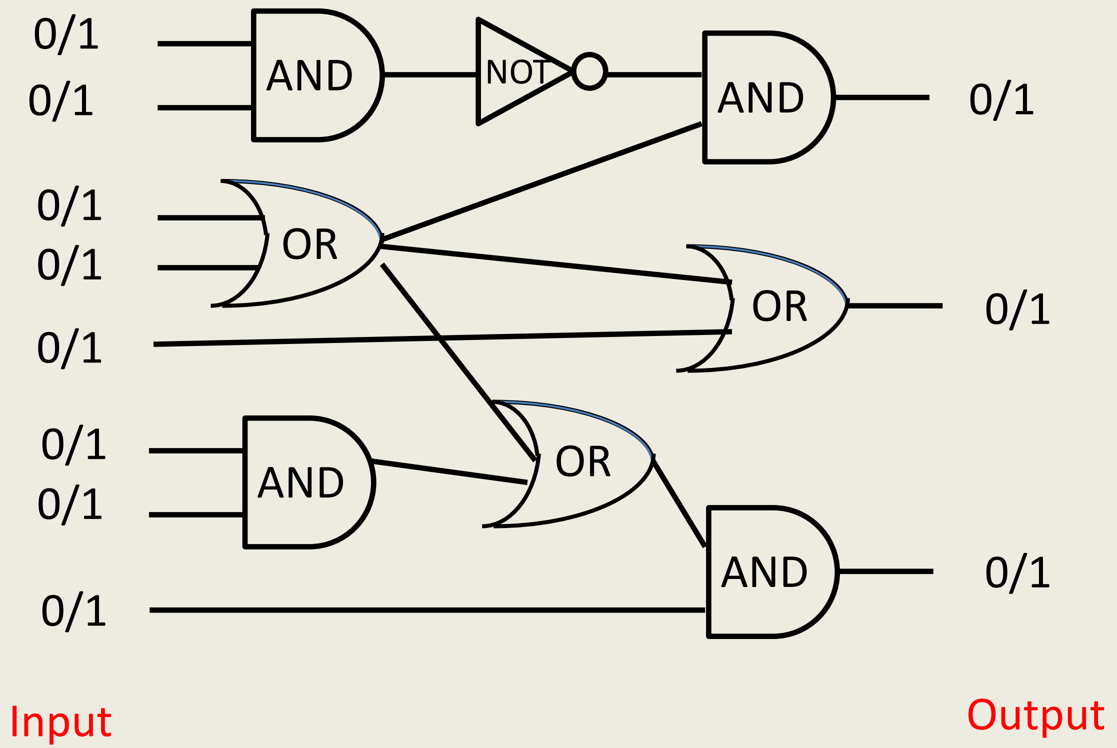
- If all n qubits are examined:
  - Outcome is
    010 with probability $|\alpha_{010}|^2$.

  - The measurement causes the state of the system to change:
    - » The state "collapses" to **010**

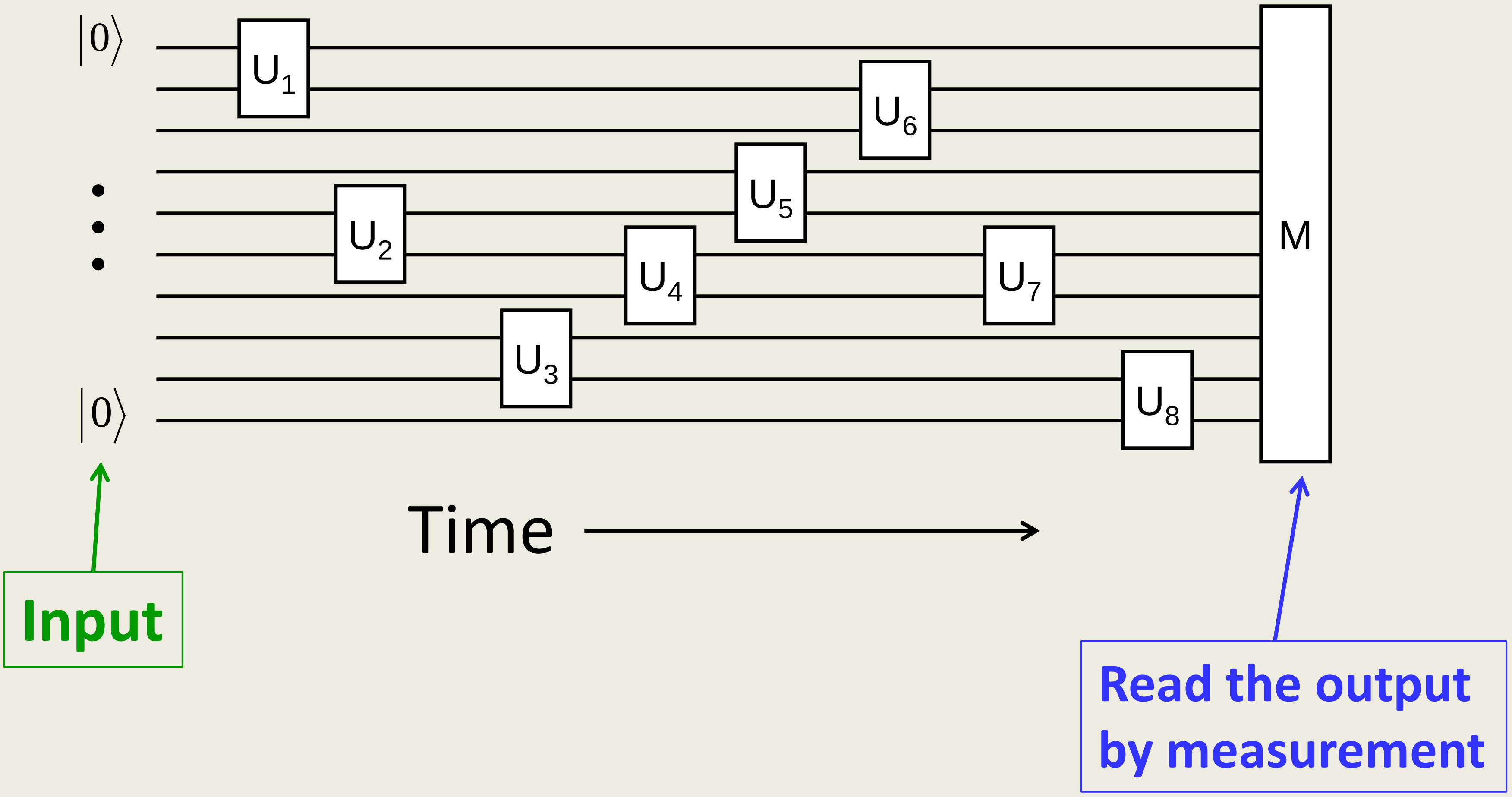
Ingredients in Computation

- Store information about a problem to be solved
- Manipulate the information to solve the problem
- Read out an answer

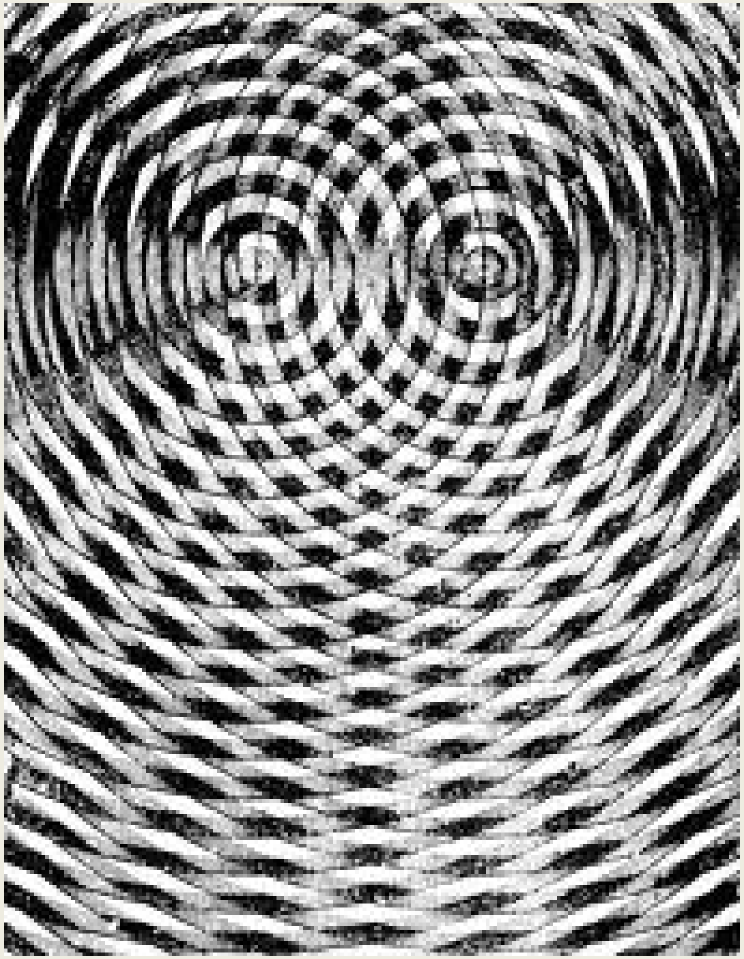
Computer Circuits



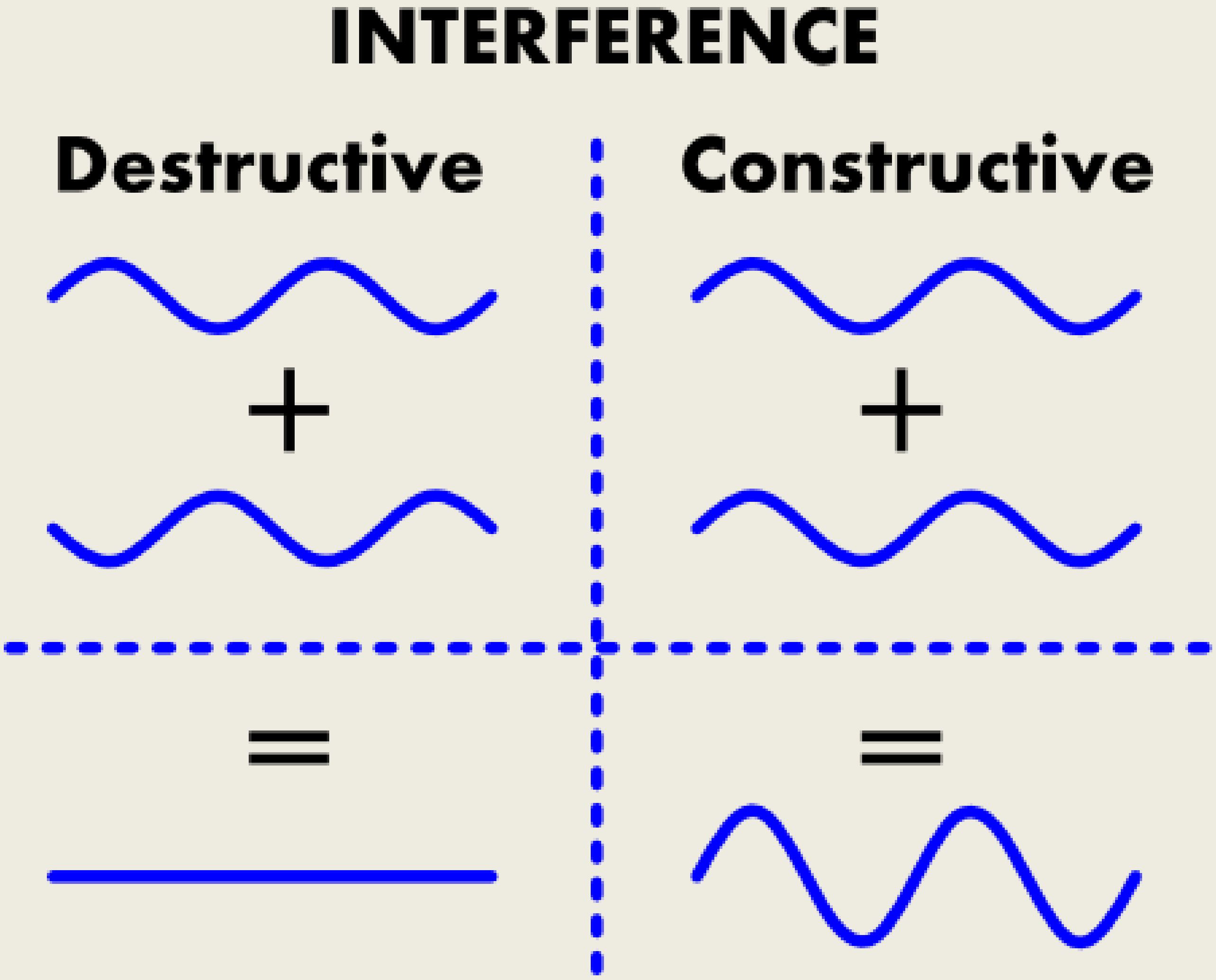
Quantum Circuits



Interference

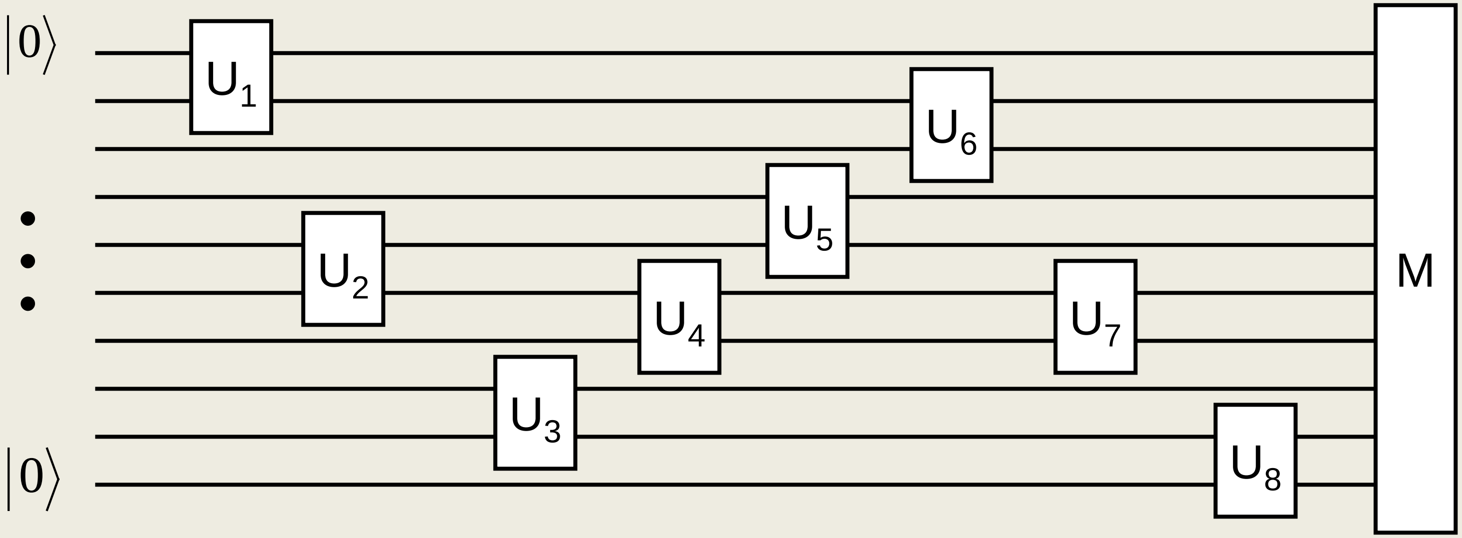


[Image from www.thehum.info, due to Dr. Glen MacPherson]



[Figure from gwoptics.org]

Quantum Circuits



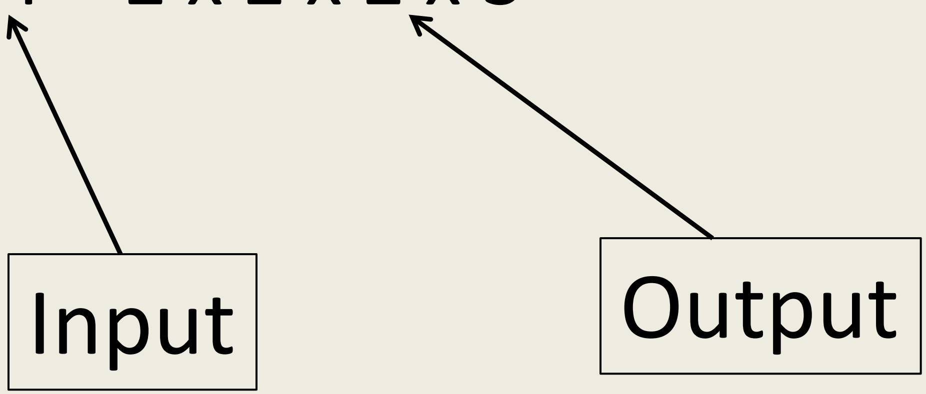
Quantum Algorithms

Manipulate data so that negative interference causes wrong answers to have small amplitude and right answers to have high amplitude, so that when we measure output, we are likely to get the right answer.

Factoring

- Given a positive integer, find its prime factorization.

- 24 = 2 x 2 x 2 x 3



Factoring

- RSA-210 = 245246644900278211976517663573088018467026787678332759743414451715061600830038587216952208399332071549103626827191679864079776723243005600592035631246561218465817904100131859299619933817012149335034875870551067

Can Quantum Computers Be Built?

- Key challenge: prevent *decoherence* (interaction with the environment).

- Can factor N=15 on a quantum computer

- Larger problems will require quantum error correcting codes.

nature

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

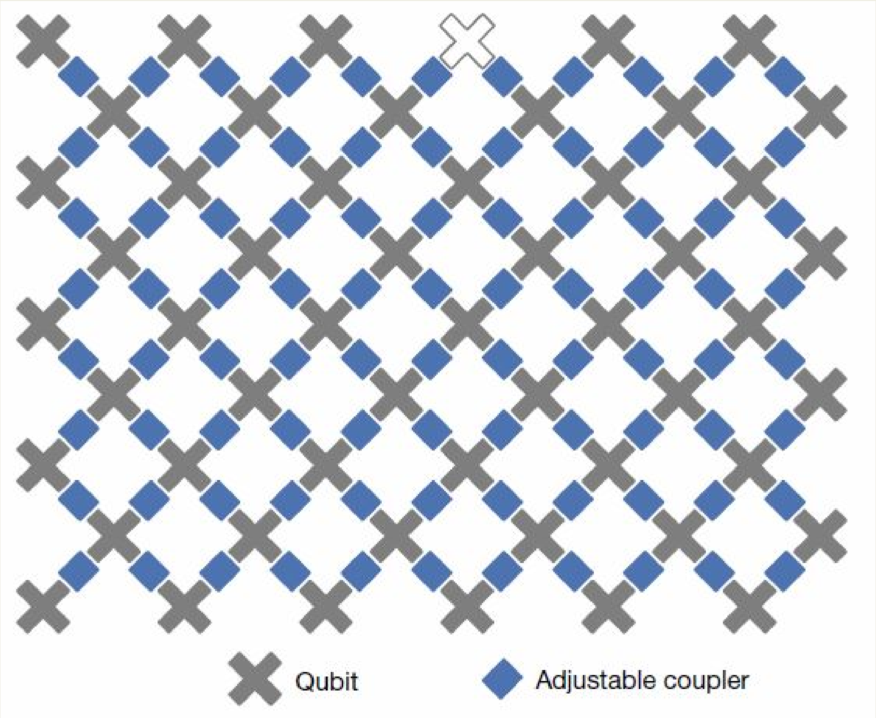
Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*

Layout of Google's "Sycamore" Quantum Processor



Picture from *Nature* Vol 574, October 24, 2019

Select a "random" quantum circuit (set of interactions)
Then repeatedly sample the outcome.
One repetition -> one 53-bit string

How Do You Check a Quantum Computer?

- Google estimated that it would take 10,000 years to check using 100,000 conventional computers running the fastest algorithms currently known.

  Simulating the 53 qubit machine requires storing

  2^{53} = 9 quadrillion = 9×10^{15} complex numbers

- Instead…check smaller versions of the same problem – still using massive amounts of computing power.

Science

Google researchers in Santa Barbara, California, say their advance may lead to near-term applications of quantum computers. ISTOCK.COM/JHVEPHOTO

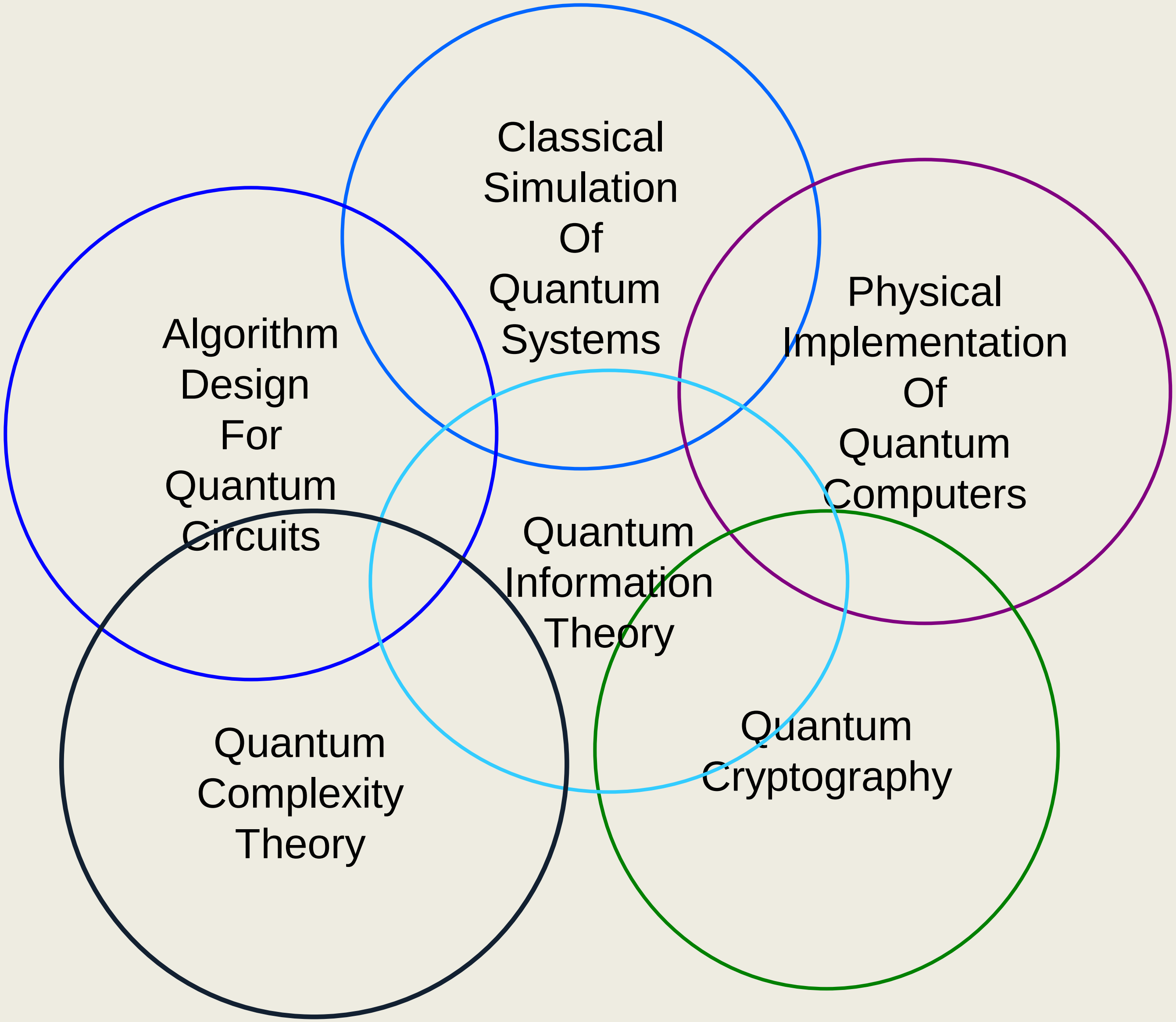
IBM casts doubt on Google's claims of quantum supremacy

By Adrian Cho | Oct. 23, 2019 , 5:40 AM

Next Steps…

- Simulate quantum physics of chemical reactions.
- Quantum error correction

Quantum Computing and Information



Research on Quantum Algorithms

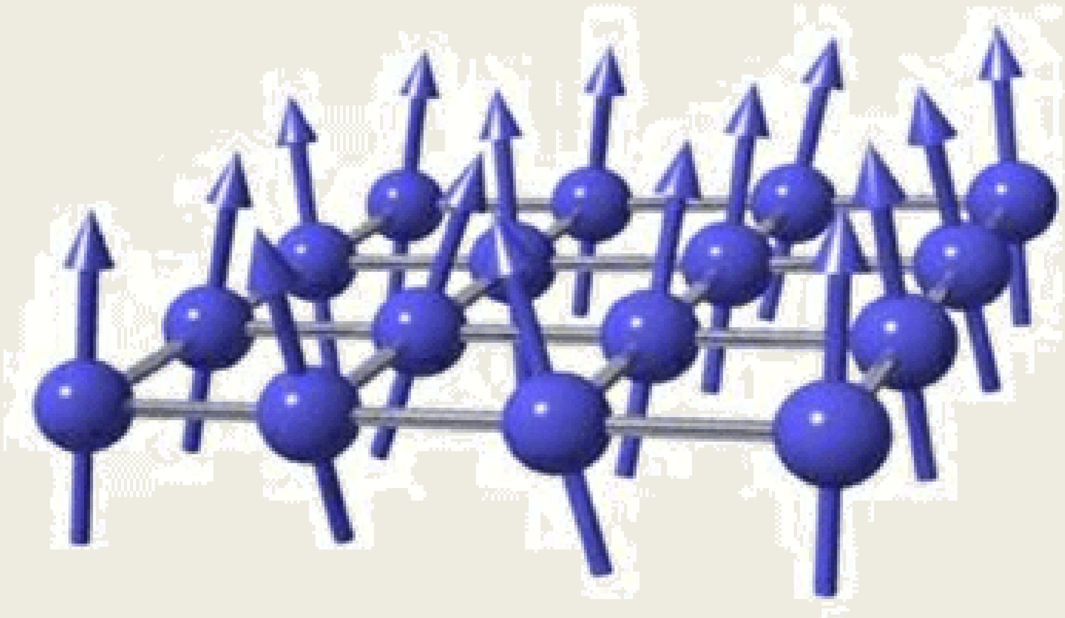
- What problems can we compute with an idealized quantum computer of the future?

  1000+ Error-Corrected Qubits

- What problems can we compute more efficiently with ~100 noisy qubits?

  NISQ computers: Near-term Intermediat-Scale Quantum Computers

Quantum Computers for Simulation in Physics



My Research

- Design efficient algorithms on a quantum (or classical) computer that will *provably* compute properties of a quantum system.
  - For what kinds of systems is this possible?
  - Or: give mathematical evidence that there is no efficient way to solve this problem.

Ways to Learn More

- CS 166 Quantum Computing

  Prerequisites:

  – Linear Algebra (ICS 6N or Math 3A)

  – Design and Analysis of Algorithms (CS 161)

- Quantum Computing Club @ UCI

  https://www.qc-uci.club