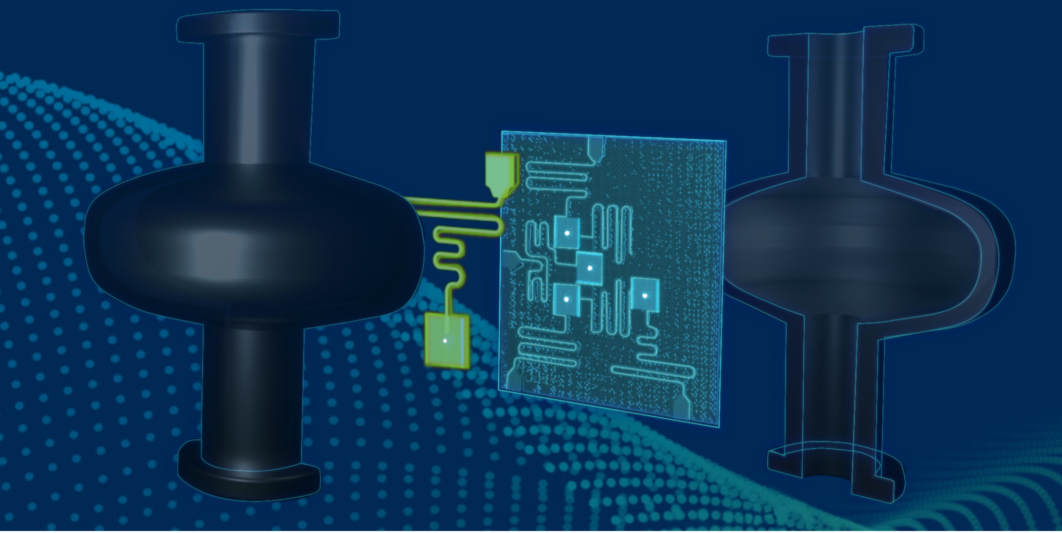
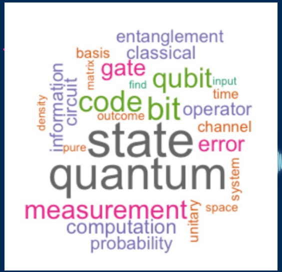
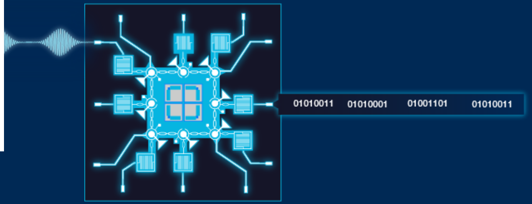






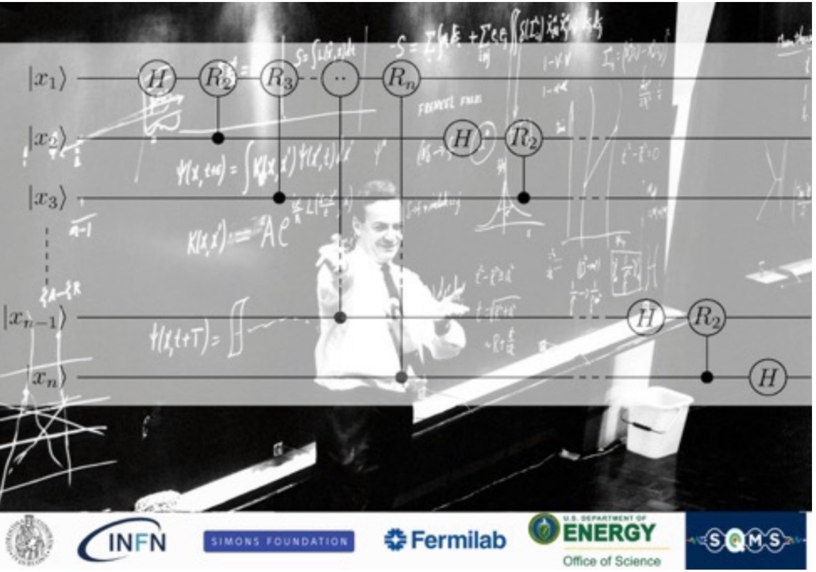
Quantum Computing:
where is it going, what is it good for?

Joe Lykken
Fermilab Quantum Institute
ACAT 2021

Quantum information science for particle physicists

"I think I can safely say that nobody understands quantum mechanics"

- Richard Feynman 1964



arXiv.org > quant-ph > arXiv:2010.02931

Quantum Physics

[Submitted on 6 Oct 2020 (v1), last revised 30 Dec 2020 (this version, v2)]

Quantum Information for Particle Theorists

Joseph D. Lykken

Lectures given at the Theoretical Advanced Study Institute (TASI 2020), 1-26 June 2020.

See my TASI school lectures for a detailed introduction to quantum information science from the point of view of particle physics

Quantum science and technology areas of active research

- **Quantum computing:** developing processors that manipulate large numbers of entangled qubits coherently

- **Quantum algorithms:** mapping interesting hard problems to quantum circuits

- **Quantum sensors:** using quantum devices as sensors, exploiting quantum properties to, e.g., detect dark matter in the laboratory

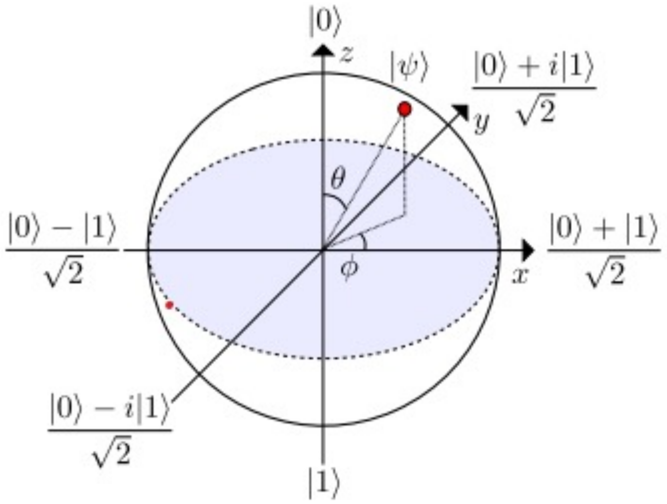
- **Quantum communications:** moving quantum information over long distances coherently, with applications to networking of quantum computers or sensors, secure communications, etc.

Quantum computing: from bits to qubits

- Information is stored and manipulated as quantum states called **qubits**
- A single qubit state is in general a **quantum superposition** of two distinct states, which we denote as state l0> and state l1>:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

- The two angles parameterize the surface of a sphere, called the Bloch sphere
- If the qubit is **entangled** with other qubits, it is described by a density matrix that maps to points in the interior of the Bloch sphere

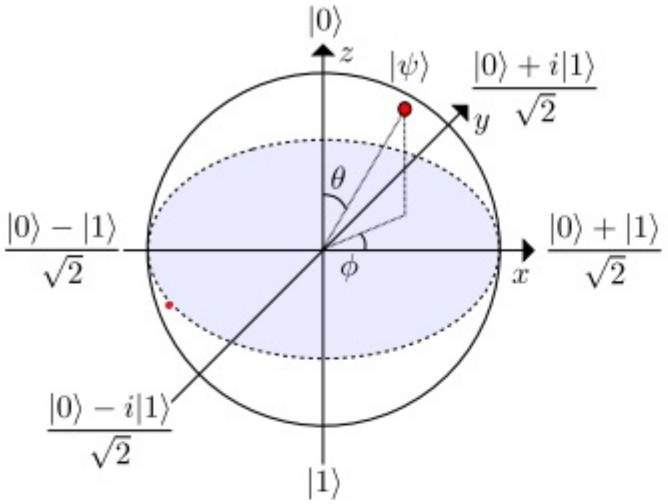


Quantum gates

- Starting from any single qubit state you can apply a unitary gate operation that rotates you to some other state on the surface of the Bloch sphere
- For example, the **Hadamard gate H** takes the I0> state to the I+> state, and takes the I1> state to the I-> state, where

$$|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



- I0> and I1> are called the **computational basis**
- I+> and I-> are called the Hadamard basis

Fermilab

Quantum entanglement

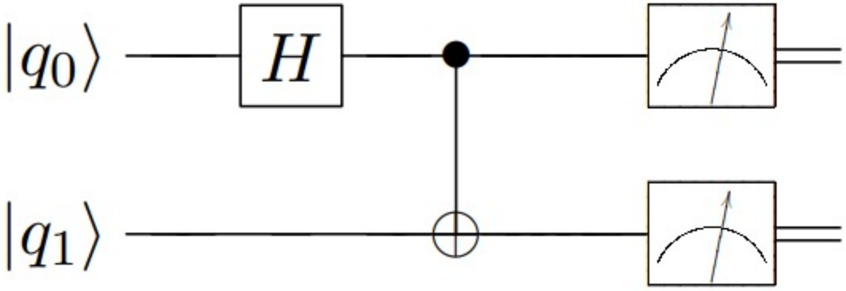
- A quantum state of two or more qubits can be **entangled**, meaning that the state cannot be written as a tensor product of single qubit states
- For two qubits a basis for entangled states is the four Bell states:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Each of these states is maximally entangled, meaning that each qubit is sharing 100% of the information about its quantum state with the other qubit

Creating entangled states in a quantum circuit

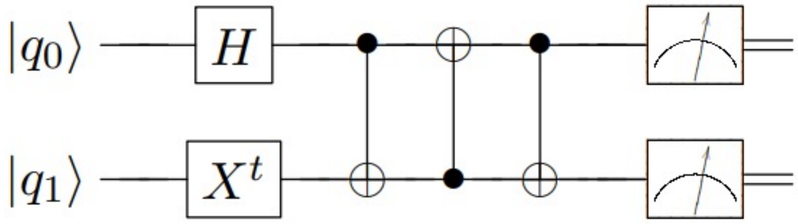
- Starting with a 2-qubit state in the computational basis, you can create a Bell state by applying the Hadamard gate and then a **CNOT**, which is a 2-qubit entangling gate



Fermilab

Swapping qubits and the no-cloning theorem

- With 3 CNOT gates you can **swap** the (arbitrary unknown) quantum states of two qubits



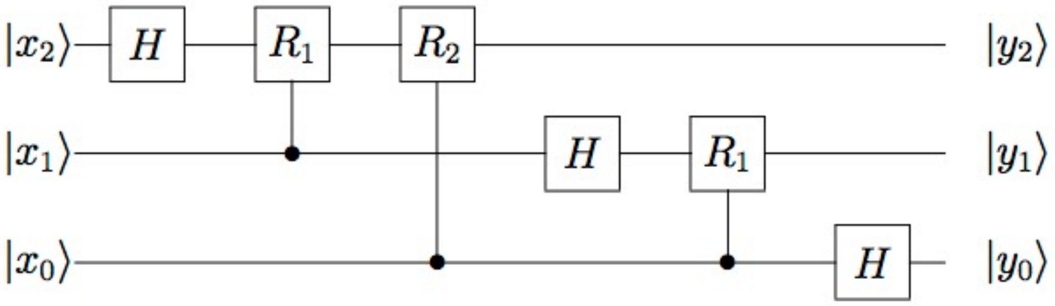
- However, the **no-cloning theorem** says that you **cannot copy** the quantum information of an (arbitrary unknown) qubit

Fermilab

Universal quantum digital computers

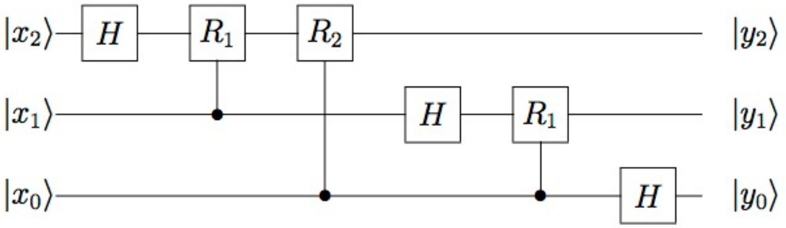
- Starting from a small menu of gates, you can obtain a **universal digital quantum computer**
- In principle can solve any problem if you have enough qubits and can apply enough gates (without errors) before **quantum decoherence** destroys your program

For example, this circuit performs a discrete Fourier transform on 3 qubits worth of information



Exponential speedup

- The discrete Fourier transform is an example of a calculation that a quantum computer can do **exponentially faster** than any classical computer:
- For n qubits we need ~ n^2 gate operations, whereas a conventional Fast Fourier Transform requires ~ $n2^n$ operations
- In 1994 Peter Shor showed that **factorization of a product of large prime numbers** can be done this way.
- Thus a quantum computer can do at least one important calculation **exponentially faster than a classical computer**
- This will eventually be the doom of **RSA encryption**



How long before quantum computers destroy the world economy?

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1,*] and Martin Ekerå[2]

[1] *Google Inc., Santa Barbara, California 93117, USA*
[2] *KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden*
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

(Dated: May 24, 2019)

We significantly reduce the cost of factoring integers and computing discrete logarithms over finite fields on a quantum computer by combining techniques from Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assu
scale superconducting qubit platforms: a planar grid of qubits with nearest-nei
a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1
reaction time of 10 microseconds. We account for factors that are normally ign
the need to make repeated attempts, and the spacetime layout of the computati
2048 bit RSA integers, our construction's spacetime volume is a hundredfold les
estimates from earlier works (Fowler et al. 2012, Gheorghiu et al. 2019). In t
model (which ignores overheads from distillation, routing, and error correction
uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n$
depth to factor n-bit RSA integers. We quantify the cryptographic implications
for RSA and for schemes based on the DLP in finite fields.

Craig Gidney giving the first ever public tutorial by Google on quantum computing software: Fermilab 9/13/18

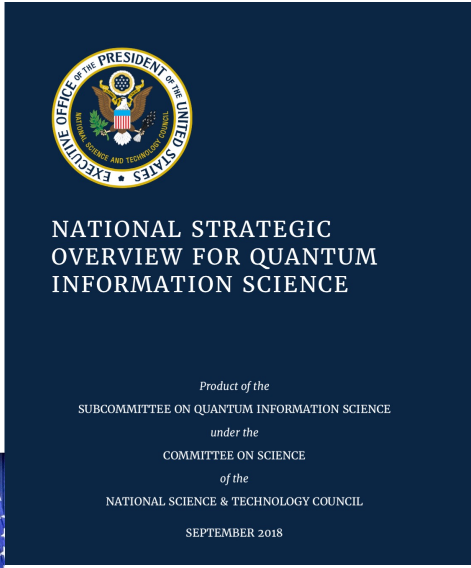
US National Quantum Initiative

In the past two years created five Dept. of Energy national quantum centers and eight NSF quantum centers

Develop quantum computers, quantum sensors, and quantum communications

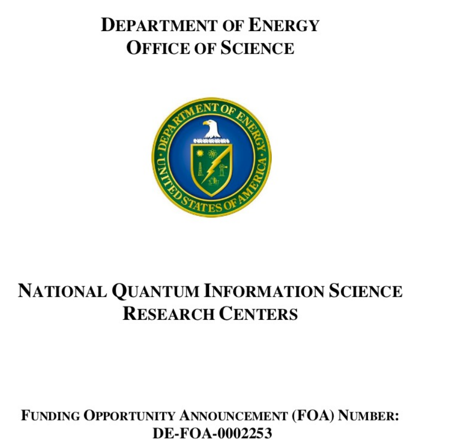
Goal is transformational advances in quantum science and technology

Create a quantum economy


NATIONAL STRATEGIC OVERVIEW FOR QUANTUM INFORMATION SCIENCE

Product of the
SUBCOMMITTEE ON QUANTUM INFORMATION SCIENCE
under the
COMMITTEE ON SCIENCE
of the
NATIONAL SCIENCE & TECHNOLOGY COUNCIL

SEPTEMBER 2018


DEPARTMENT OF ENERGY
OFFICE OF SCIENCE

NATIONAL QUANTUM INFORMATION SCIENCE RESEARCH CENTERS

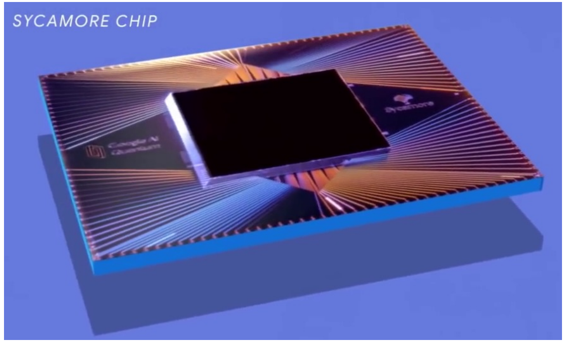
FUNDING OPPORTUNITY ANNOUNCEMENT (FOA) NUMBER:
DE-FOA-0002253

SQMS National Quantum Research Center @Fermilab

Using Fermilab expertise in superconducting materials and systems to build better quantum computers

Quantum "Supremacy"

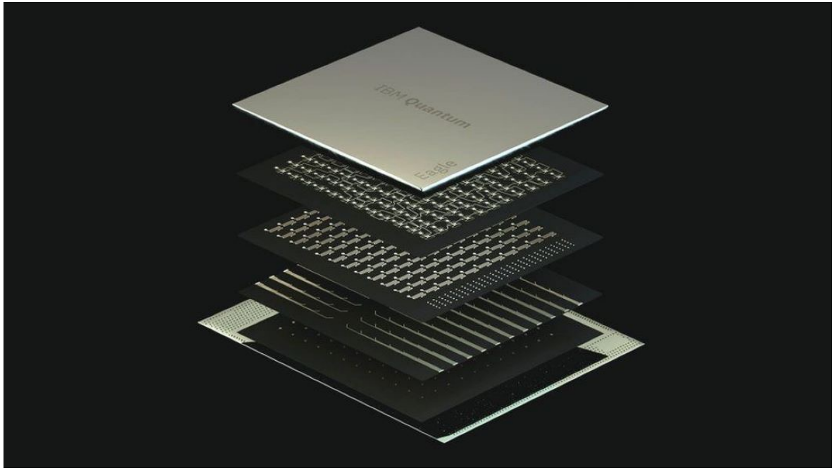
Google paper in 2019 reported how their 53-qubit superconducting Sycamore quantum processor outperformed Summit, the largest US supercomputer, on a particular task



Rapid progress, big challenges

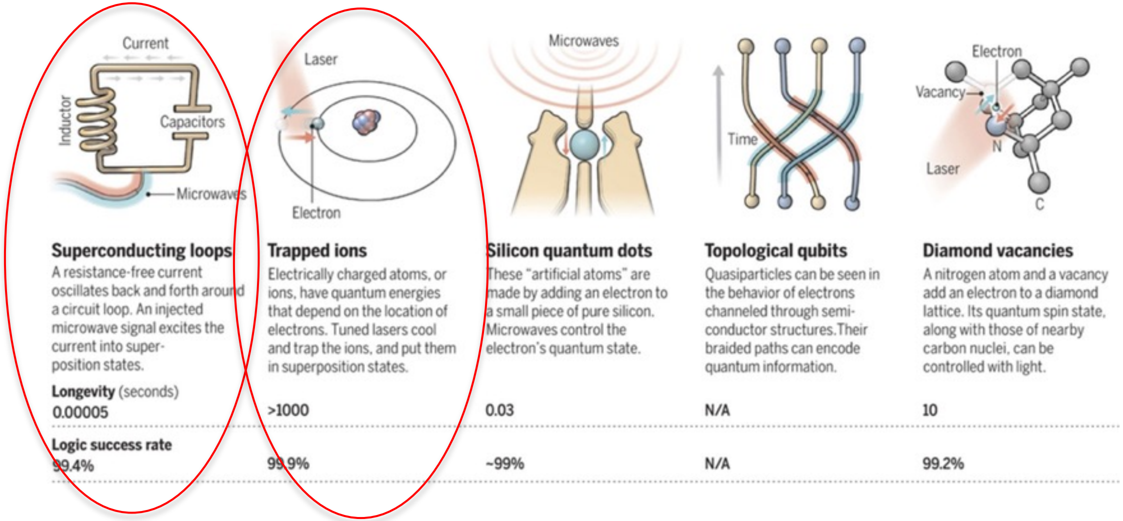
- IBM has just announced their 127-qubit processor Eagle

- Plans to get to 1000 qubits and beyond using interconnected dilution fridges



- Hybrid classical-quantum cloud services are under development by several companies

Private sector placing big bets on qubits



"The tech giants, IBM , Google , and Intel , all have staked out their quantum computing claims with superconducting qubits. Rigetti Computing, a recent but impressive California start-up, also uses superconducting qubits"

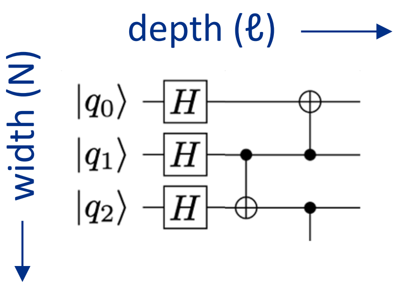
Qubit technologies overview. From: Forbes, *Quantum Computer Battle Royale: Upstart Ions Versus Old Guard Superconductors*

Commercially deployed quantum processors so far use either superconducting microwave circuits (IBM, Google, Rigetti) or trapped ions (IonQ, Honeywell)

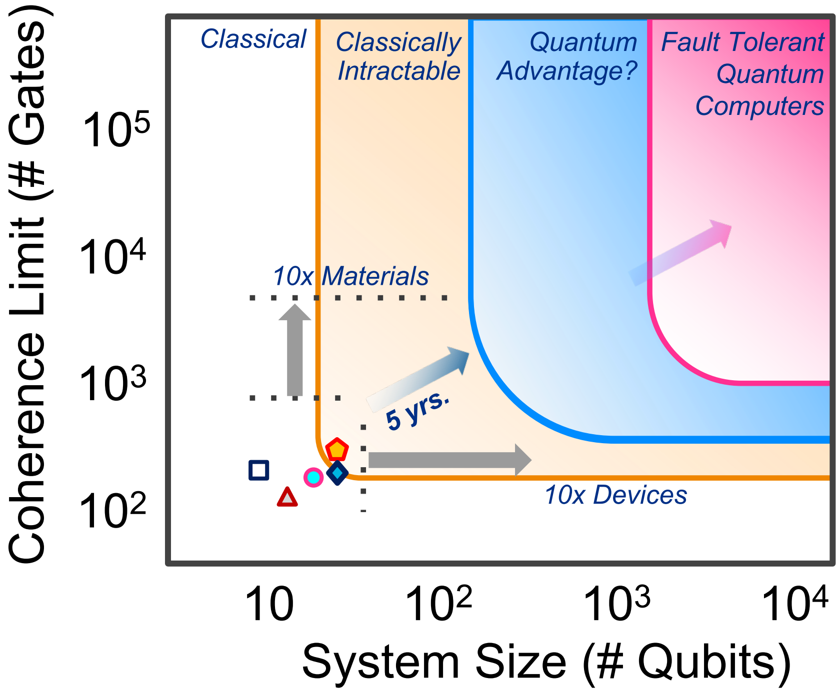
US now has more private investment in quantum technology than government funding

Quantum computing: the road to Quantum Advantage

Quantum algorithms:



Superconducting Qubits



Fermilab

So: what are quantum computers actually good for?

“Quantum advantage” refers to any case where a quantum processor provides a **useful** advantage in tackling an **important** problem (or part of an important problem)

This is not the same thing as asking for exponential speedup, since for some problems a 20% improvement is a big deal

And it is more than an algorithmic question:

- How much do you care about about noise/errors?
- How much do you care about where the processor is deployed, or how fast is the turn around time?

Obviously subject matter experts, e.g. scientists, need to be directly involved in developing use cases with validated quantum advantage

Seeking quantum advantage

Applications of quantum computing for particle physics, nuclear, etc

This talk: quantum simulations of HEP/NP physical systems

Real-time strong dynamics:
- Neutrino-nuclear interactions

Real-time non-equilibrium dynamics:
- Cosmological phase transitions

Quantum gravity
- Wormholes

Practical Quantum Advantages in High Energy Physics

Marcela Carena,[1,2,3,*] Henry Lamm,[1,†] Scott Lawrence,[4,‡] Ying-Ying Li,[1,§] Joseph D. Lykken,[1,¶] Lian-Tao Wang,[2,**] and Yukari Yamauchi[5,††]

Snowmass 2021 LOI TF10-077 (2020)

Other important applications (much broader than HEP/NP):

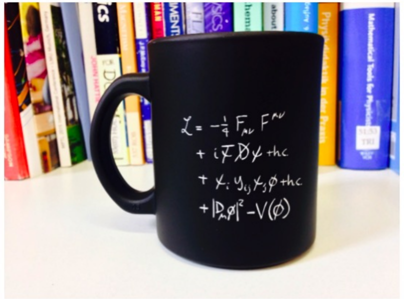
- Quantum AI/ML (see ACAT talk by Barry Sanders)
- Quantum optimization
- etc

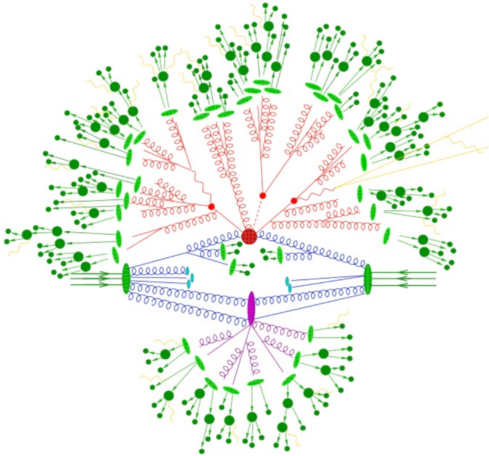
Real time strong dynamics

Consider proton-proton collisions at the LHC:

- We know the underlying theory is QCD
- But even with the largest classical supercomputers we must instead resort to modeling and data-extracted parton distributions

- No one is even ***attempting*** to compute real-time QCD dynamics
- Why?





See ACAT talk by Anja Butter

The Sign Problem

It is a basic physics fact that the nonperturbative real-time evolution of quantum fields has a sign problem:

$$\langle O \rangle = \frac{\sum_{\mathcal{C}} O(\mathcal{C}) W(\mathcal{C})}{\sum_{\mathcal{C}} W(\mathcal{C})}$$

$$\text{Imaginary time problem}: W(\mathcal{C}) \sim \exp(-S(\mathcal{C}))$$

$$\text{Real time problem}: W(\mathcal{C}) \sim \exp(iS(\mathcal{C}))$$

- Problems that can be formulated in imaginary time are computationally tractable by going to a discrete space-time lattice = **Lattice Gauge Theory**
- But for real-time problems the relevant discretized configuration space is **exponentially large** compared to the lattice size

As Feynman first observed, we need to use quantum computers to solve quantum problems

The Sign Problem

It is a basic physics fact that the nonperturbative real-time evolution of quantum fields has a sign problem:

$$\langle O \rangle = \frac{\sum_{\mathcal{C}} O(\mathcal{C}) W(\mathcal{C})}{\sum_{\mathcal{C}} W(\mathcal{C})}$$

$$\text{Imaginary time problem} : W(\mathcal{C}) \sim \exp(-S(\mathcal{C}))$$

$$\text{Real time problem} : W(\mathcal{C}) \sim \exp(iS(\mathcal{C}))$$

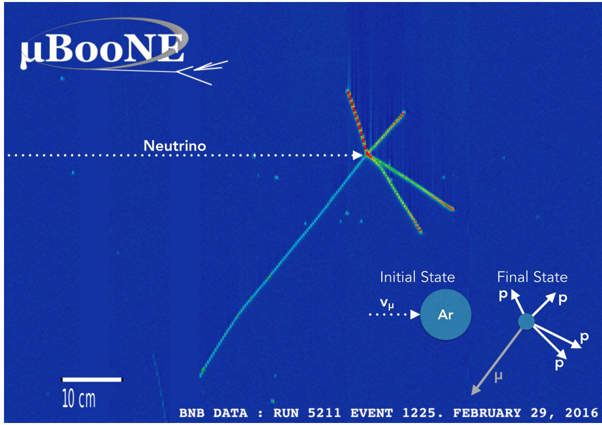
- Particle and nuclear physics today derive great benefit from developments in lattice gauge theory that began decades ago, **long before** petascale computers became available to do the actual simulations
- **A similar program has now started for quantum computing**

Quantum computing for neutrino discoveries

As the recent MicroBooNE results show, we have entered a new era of neutrino physics enabled by the capabilities of Liquid Argon Time Projection Chambers

- But this means we care about the details of how the argon nucleus rattles around after being struck by a neutrino
- This is a physics challenge where quantum computers may be part of the solution

- And we should have pretty good quantum computers by the 2030's when the DUNE experiment is running



P. Abratenko *et al.* (MicroBooNE Collaboration)
Phys. Rev. Lett. 123, 131801

arXiv.org > quant-ph > arXiv:1911.06368

Quantum Physics

[Submitted on 14 Nov 2019]

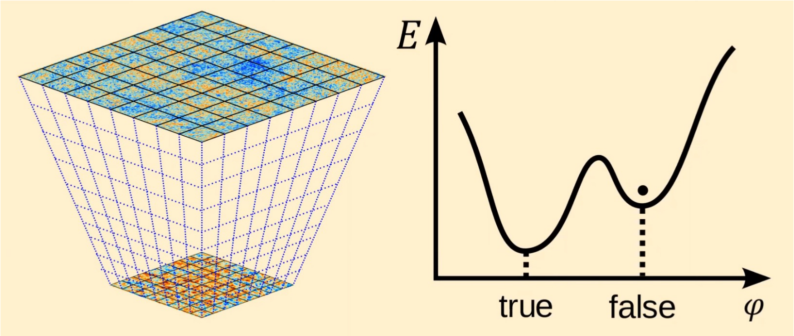
Quantum Computing for Neutrino-nucleus Scattering

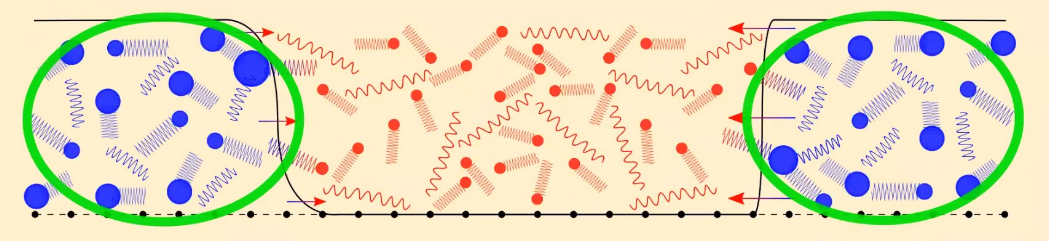
Alessandro Roggero, Andy C. Y. Li, Joseph Carlson, Rajan Gupta, Gabriel N. Perdue

Quantum computing for cosmological phase transitions

For example, it may be that matter dominates over antimatter in our universe because of a baryogenesis process during a first order phase transition in the early universe:

- This involves nonequilibrium, nonadiabatic, nonperturbative dynamics in curved spacetime
- Bubbles of the new vacuum nucleate, interact, and merge to complete the phase transition



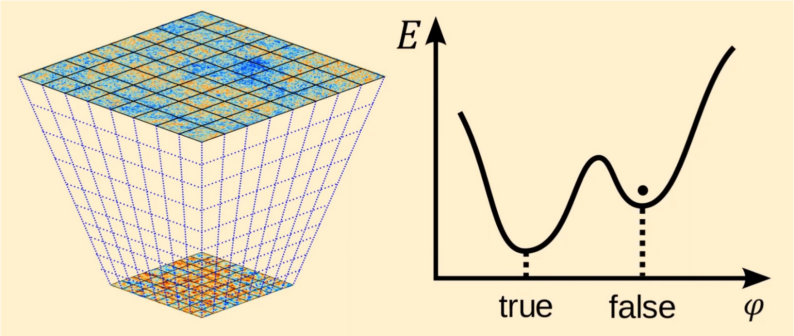


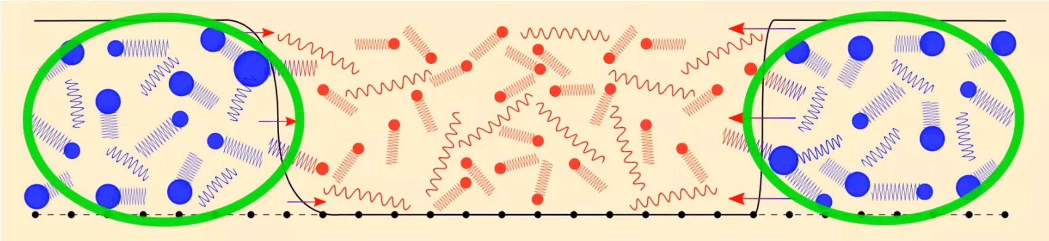
Slides from Hank Lamm

Quantum computing for cosmological phase transitions

For example, it may be that matter dominates over antimatter in our universe because of a baryogenesis process during a first order phase transition in the early universe:

- Baryogenesis cares about the details of this dynamics
- This is a physics challenge where quantum computers may be part of the solution





arXiv.org > quant-ph > arXiv:2012.07243

Quantum Physics

[Submitted on 14 Dec 2020 (v1), last revised 9 Mar 2021 (this version, v2)]

Collisions of false-vacuum bubble walls in a quantum spin chain

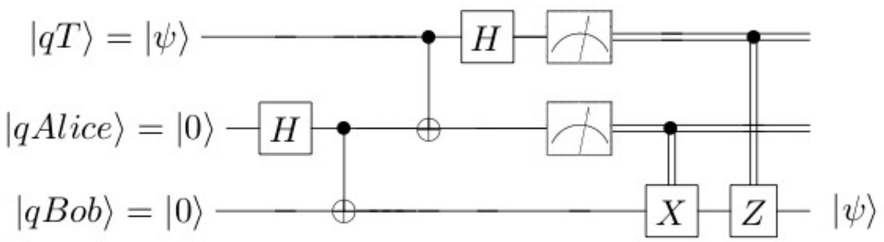
Ashley Milsted, Junyu Liu, John Preskill, Guifre Vidal

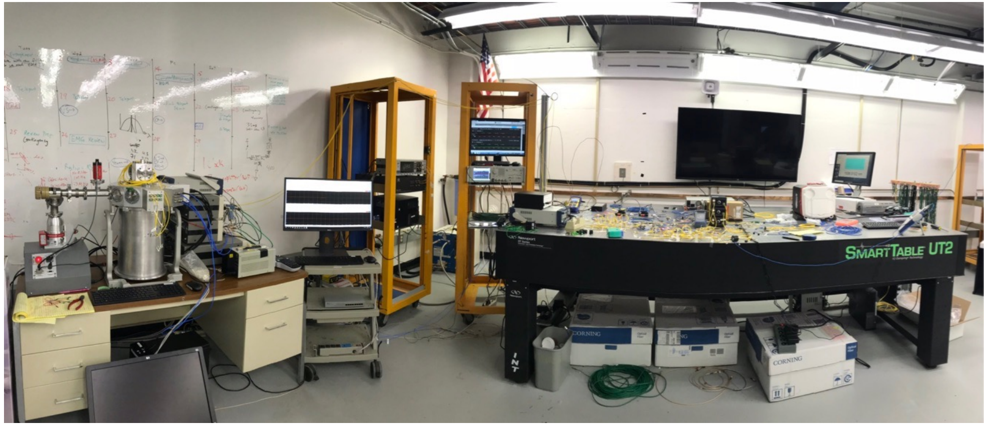
Slides from Hank Lamm

Wormhole teleportation

An example of the possibility of doing quantum gravity in the laboratory

- Quantum teleportation is something we know how to do in a lab
- It involves moving quantum information (an unknown superposition state) from one place to another





The first node of the Fermilab Quantum Network

Wormhole teleportation

- In 2016 Gao, Jafferis and Wall showed that the physical systems can contain a traversable **wormhole** when perturbed in a particular way
- In 2019 Gao and Jafferis wrote an explicit protocol for **quantum teleportation** that in a dual picture maps to a traversable wormhole

P. Gao, D. Jafferis, “A traversable wormhole teleportation protocol in the SYK model”, arXiv:1911.07416

- In one physical picture quantum information disappears then reappears somewhere else because it is scrambled, teleported, then unscrambled
- While in the equivalent dual picture **it disappears into a wormhole then re-emerges**

Daniel Jafferis explaining wormhole teleportation at the Kavli Aspen quantum workshop, May 2019

Outlook

- In the case of Lattice Gauge Theory, theoretical advances (e.g. improved actions) made orders of magnitude improvement in our ability to do important HEP/NP calculations on classical computers
- I predict that the same thing will happen with quantum, thus advancing the time when quantum computers will make important contributions to our science
- This is and will continue to be an exciting area to work in

arXiv.org > hep-lat > arXiv:2107.01166

High Energy Physics – Lattice

[Submitted on 2 Jul 2021 (v1), last revised 27 Jul 2021 (this version, v2)]

Lattice Renormalization of Quantum Simulations

Marcela Carena, Henry Lamm, Ying-Ying Li, Wanqiang Liu