Introduction to Quantum Computing I

Eleanor G. Rieffel

NASA Senior Researcher for Advanced Computing and Data Analytics

NASA Ames Quantum Artificial Intelligence Laboratory (QuAIL) Lead

August 7, 2023

Why Quantum Computing at NASA?

NASA constantly confronts massively challenging computational problems

Computational capacity limits mission scope and aims

Pleiades supercomputer at NASA Ames

NASA QuAIL mandate: ***Determine the potential for quantum computation to enable more ambitious and safer NASA missions in the future***

Quantum computing has the potential to provide vastly more efficient computation for some applications

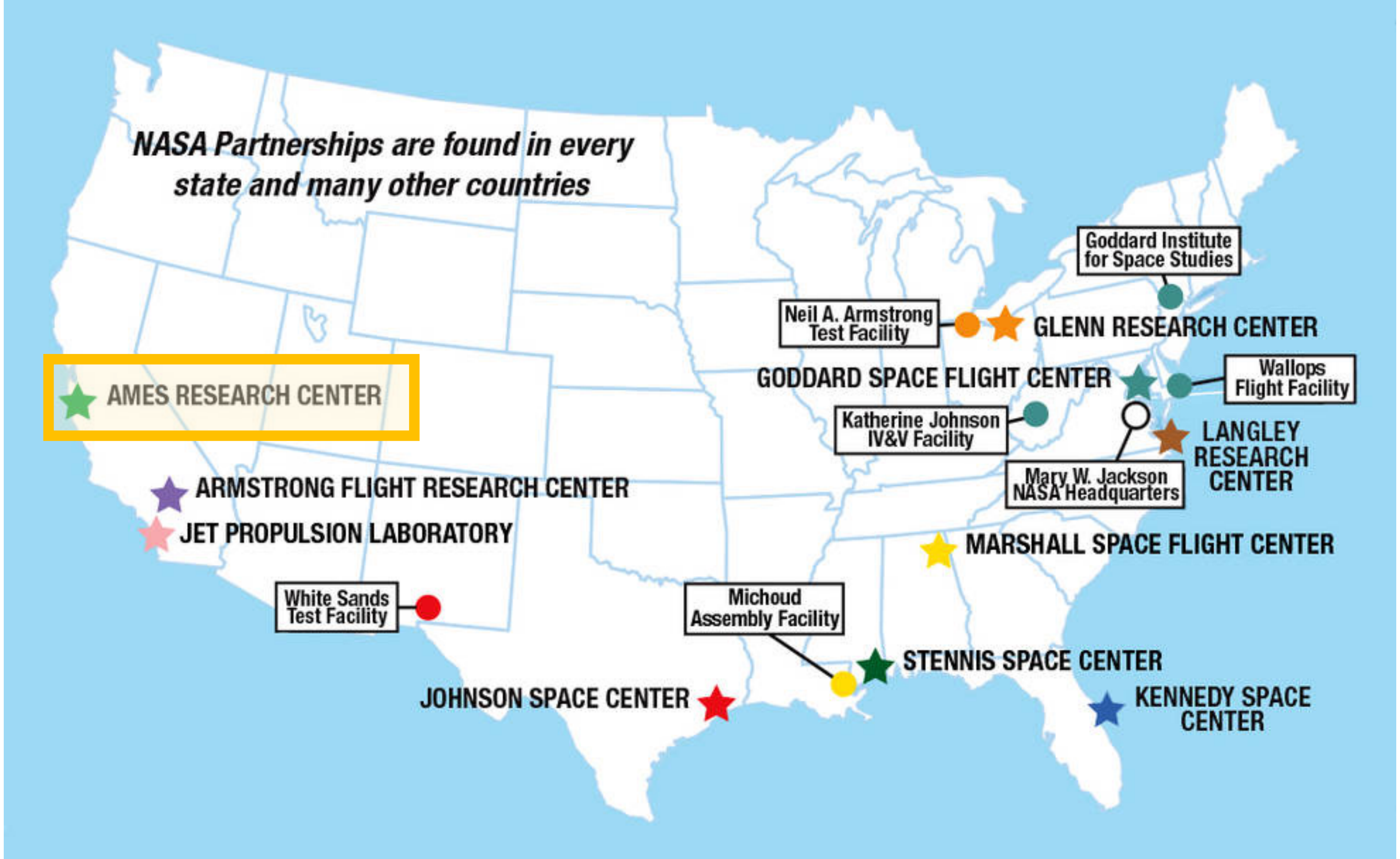
- Ability to compute what could not be computed even if every atom in the universe were a classical processor running for the entire age of the universe
  - e.g., factoring, certain material science applications
- Significant speedups in other areas such as optimization, machine learning
- Harnesses uniquely quantum effects

Green computation

- Low energy consumption

NASA Ames Research Center

Quantum Artificial Intelligence Laboratory (QuAIL) at NASA Ames



Entering Exciting New Era for Quantum Computing

Quantum advantage achieved

- Perform computations not possible on even largest supercomputers in reasonable time
- Google – NASA – ORNL collaboration

F. Arute *et al.* (2019), Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505-510

2023 Update

*A. Morvan, B. Villalonga, X. Mi, **S. Mandrà**, et al., (2023) Phase transition in Random Circuit Sampling, arXiv:2304.11119*

Exp.	1 amp.	1 million noisy samples		
	FLOPs	FLOPs	XEB fid.	Time
SYC-53 [9]	$6.44 \cdot 10^{17}$	$2.60 \cdot 10^{17}$	$2.24 \cdot 10^{-3}$	6.18 s
ZCZ-56 [10]	$6.24 \cdot 10^{19}$	$6.40 \cdot 10^{19}$	$6.62 \cdot 10^{-4}$	25.3 min
ZCZ-60 [11]	$1.32 \cdot 10^{21}$	$1.41 \cdot 10^{23}$	$3.66 \cdot 10^{-4}$	38.7 days
This work	$4.74 \cdot 10^{23}$	$6.27 \cdot 10^{25}$	$1.68 \cdot 10^{-3}$	47.2 yr

… but so far only for a toy problem

- Quantum hardware currently too small and non-robust for solving practical problems intractable on classical supercomputers
- These devices need to scale up and become more reliable

Bad news: Advances needed before quantum computing can aid with practical problems

Good news: Lots of research opportunities, hardware, tools, algorithms …

Unprecedented opportunity to invent, explore, and evaluate quantum algorithms <u>empirically</u>

Current status of quantum algorithms

Quantum computing can do everything a classical computer can do

and

Provable quantum advantage known for a few dozen quantum algorithms

Unknown quantum advantage for everything else

Status of classical algorithms

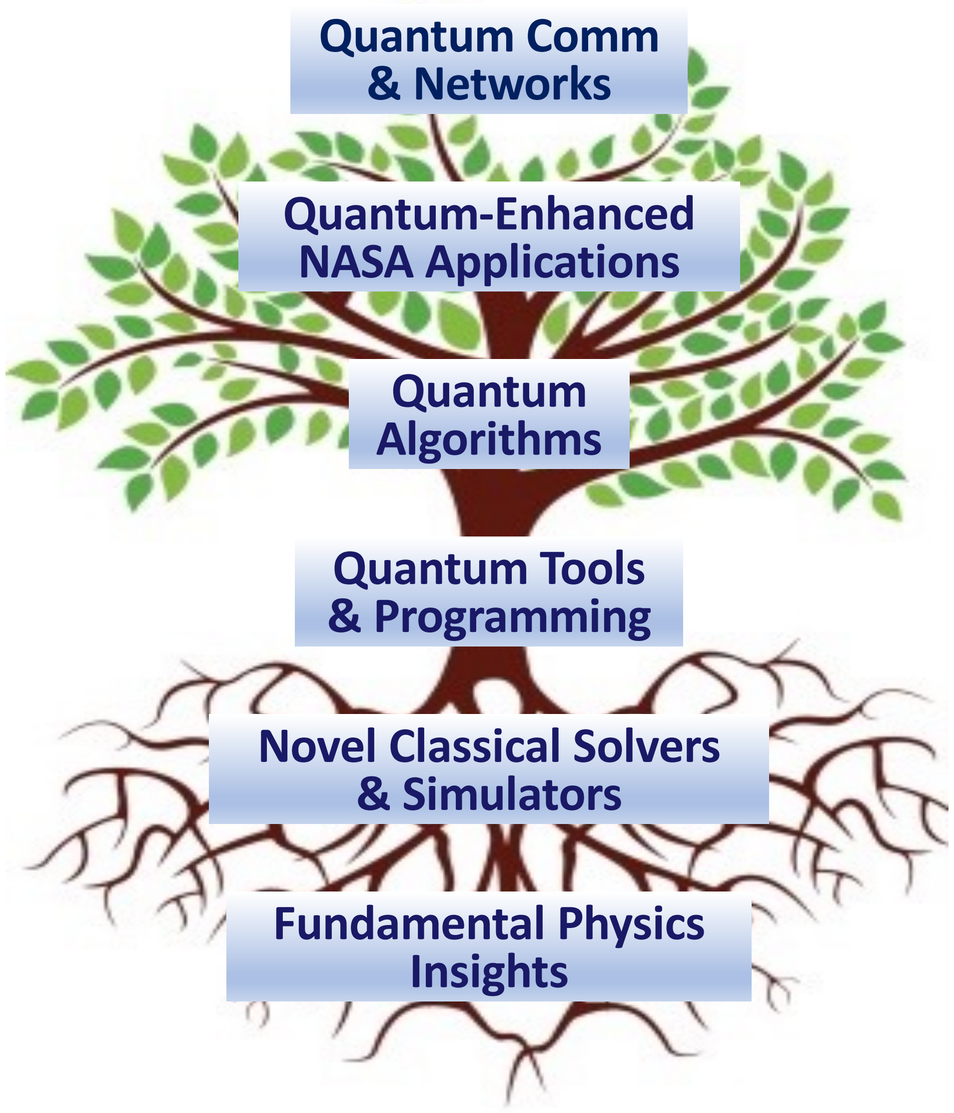
- Provable bounds hard to obtain
  - Analysis is just too difficult
- Best classical algorithm not known for most problems
- Empirical evaluation required
- Ongoing development of classical heuristic approaches
  - Analyzed empirically: ran and see what happens
  - E.g. SAT, planning, machine learning, etc. competitions

A handful of proven limitations on quantum computing

Conjecture: Quantum Heuristics will significantly broaden applications of quantum computing

Quantum Computing: NASA Ames QuAIL Team

INTELLIGENT SYSTEMS DIVISION



Communication & Networks

Quantum networking — Distributed QC

Application Focus Areas

Planning and scheduling — Material science

Logistics — Machine learning

Software Tools & Algorithms

Quantum algorithm design — Compiling to hardware

Mapping, parameter setting, error mitigation

Hybrid quantum-classical approaches

Solvers & Simulators

Physics-inspired classical solvers

HPC quantum circuit simulators

Physics Insights

Co-design quantum hardware

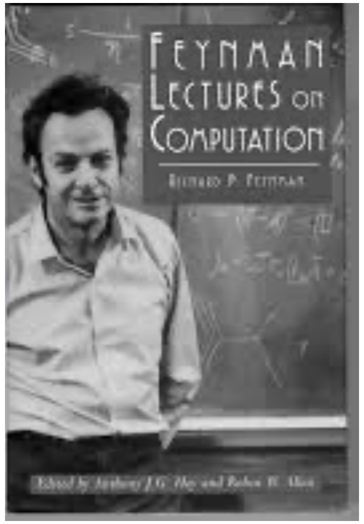
History and Background

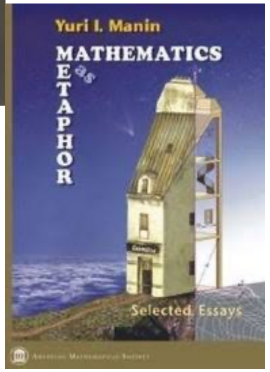
Birth of Quantum Computing

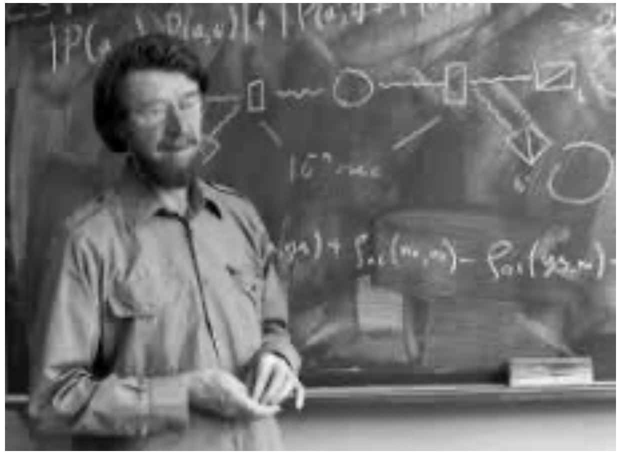
Feynman and Manin recognized in the early 1980s that certain quantum phenomena could not be simulated efficiently by a computer

- Phenomena related to quantum entanglement; Bell's inequality

Perhaps these quantum phenomena could be used to speed up more general computation?







Computers as Classical Mechanical Machines

Babbage's analytical engine was a classical mechanical machine

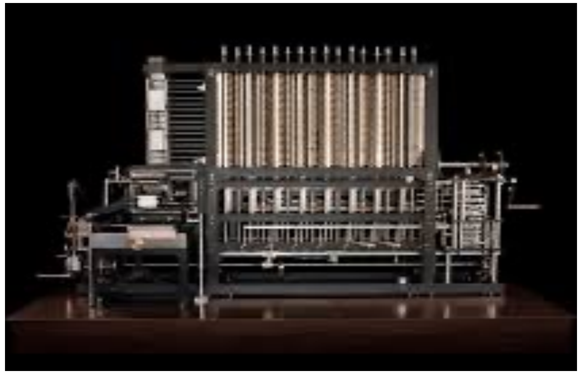
Turing machines

- The abstraction that underlies complexity theory and universal computing machines
- Firmly rooted in classical mechanics
- Described in classical mechanical terms

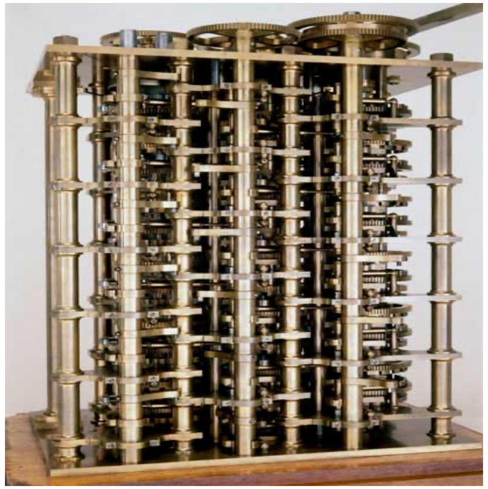
Abstraction allowed us ignore how classical computers are implemented physically

- When we program we don't think about the fundamental physics

How do different models of physics affect how quickly we can compute?



Babbage engine (Computer History Museum)



Fundamental questions

How do different models of physics affect how quickly we can compute?

- Suggests new computation-based physics principles

How would basing computation on a quantum mechanical model rather than a classical mechanical model change our notions of computing?

- Quantum physics is the physics of our universe

How quickly does nature allow us to compute?

What a Quantum Computer is Not

Just because a computer uses quantum effects, does not mean it is a Q Computer

- All the computers in this building make use of quantum effects
- The fundamental unit of computation, the bit, and the algorithms we design for computers did not change when quantum effects were used

A Quantum Computer has a fundamentally different way of encoding and processing information

- Quantum computers are quantum information processing devices
- They process qubits instead of bits
- They use quantum operations instead of logic gates

Also, just because a piece of hardware has a certain number of qubits, it isn't necessarily a Quantum Computer

- A set of light switches, even a very large set, is not a classical computer

Certainty and Randomness in Quantum Computation

Any computation a classical computer can do, a quantum computer can do with roughly the same efficiency

- With the same probability of the outcome
- If the classical computation is non-probabilistic, so is the quantum one

Like classical algorithms, some quantum algorithms are inherently probabilistic and others are not

- First quantum algorithms were not probabilistic
  - E.g. Deutsch-Jozsa algorithm solves problem with certainty that classical algorithms, of equivalent efficiency, could solve only with high probability
- Shor's algorithms are probabilistic
- Grover's is not intrinsically probabilistic
  - initial search algorithm was probabilistic, but
  - slight variants, which preserve the speed up, are non-probabilistic

Pool of quantum properties

- Quantum interference
- Quantum entanglement
- Quantum tunneling
- Quantum sampling
- Quantum measurement
- Non-commutative quantum operators
- Quantum population transfer
- Quantum many-body delocalization
- Quantum no cloning theorem
- Quantum adiabatic theorem
- Quantum discord

The power of quantum computation comes from encoding information in a non-classical way

Quantum computers take advantage of quantum effects not available classically

These effects can provide more efficient computation and higher levels of security than is available classically

- **What Shor's factoring algorithm can compute in days, would take a supercomputer longer than the age of the universe**
- **Breaks all public key encryption in standard use**

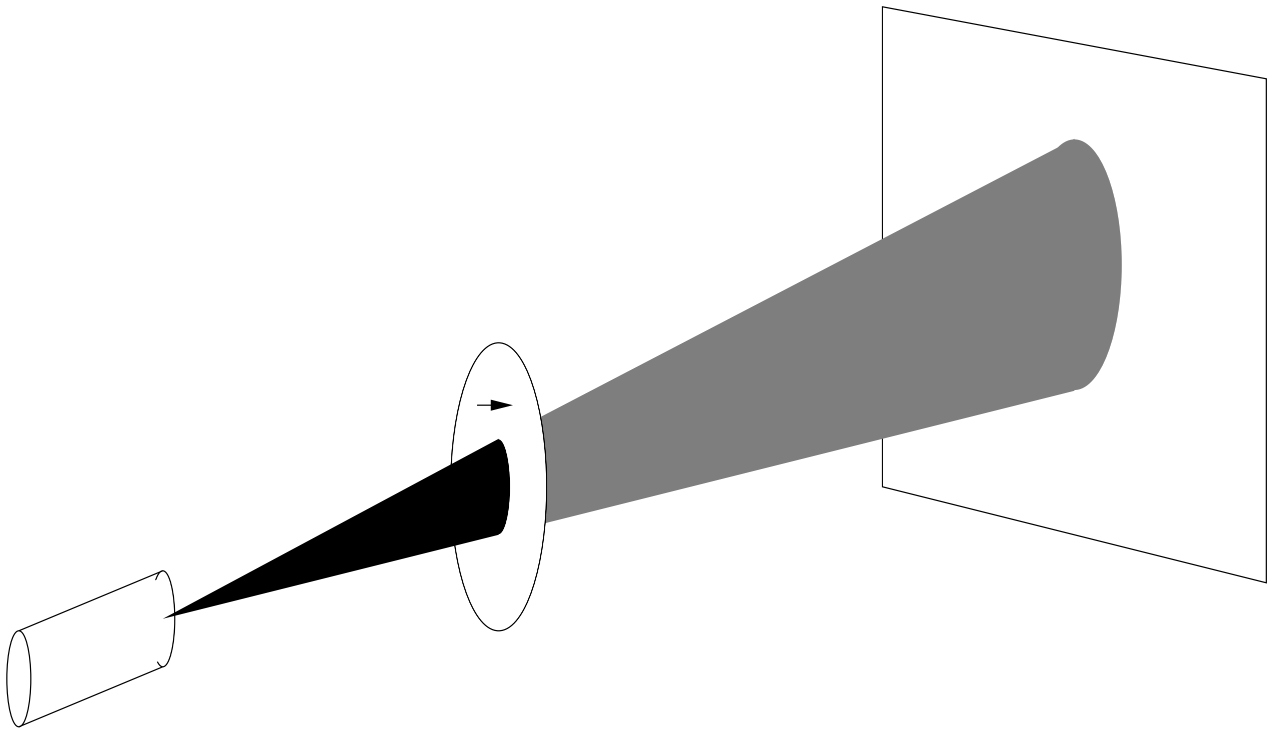
The art of quantum algorithm design is figuring out how to harness peculiarly quantum properties for computational purposes

Basic Concepts for Quantum Computing

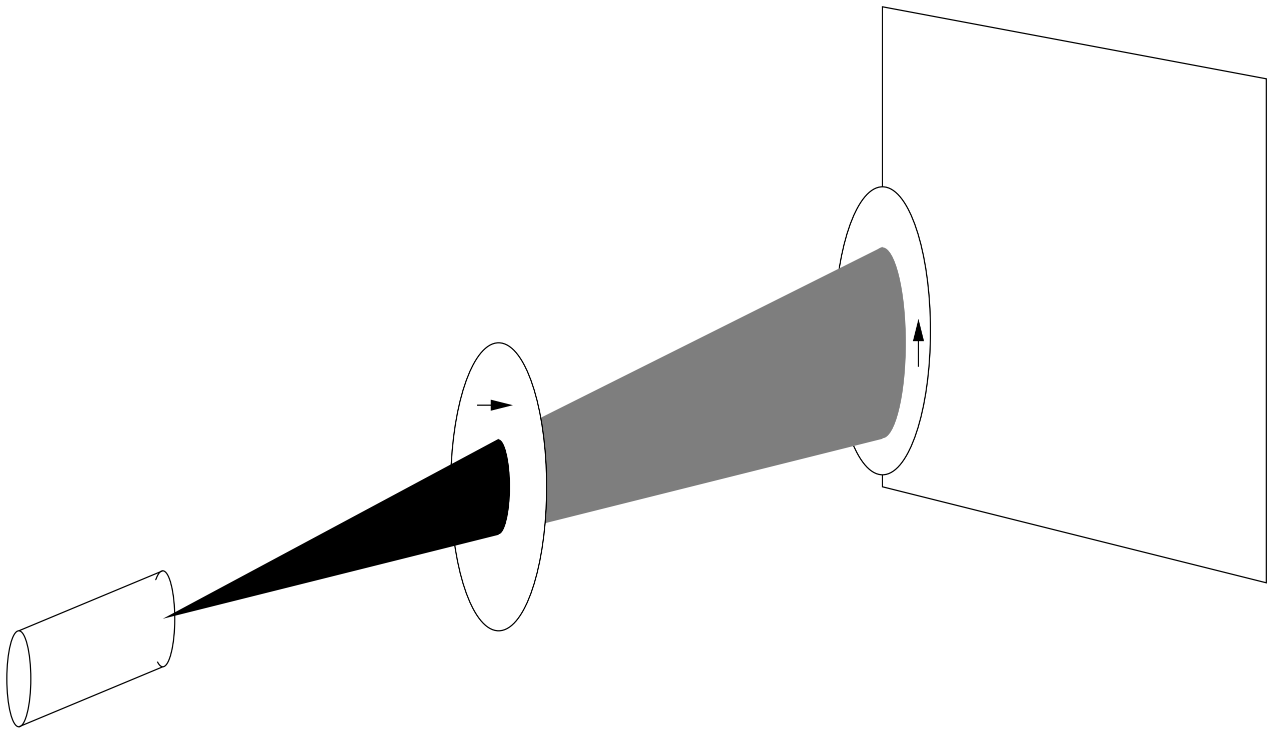
NASA

INTELLIGENT SYSTEMS DIVISION

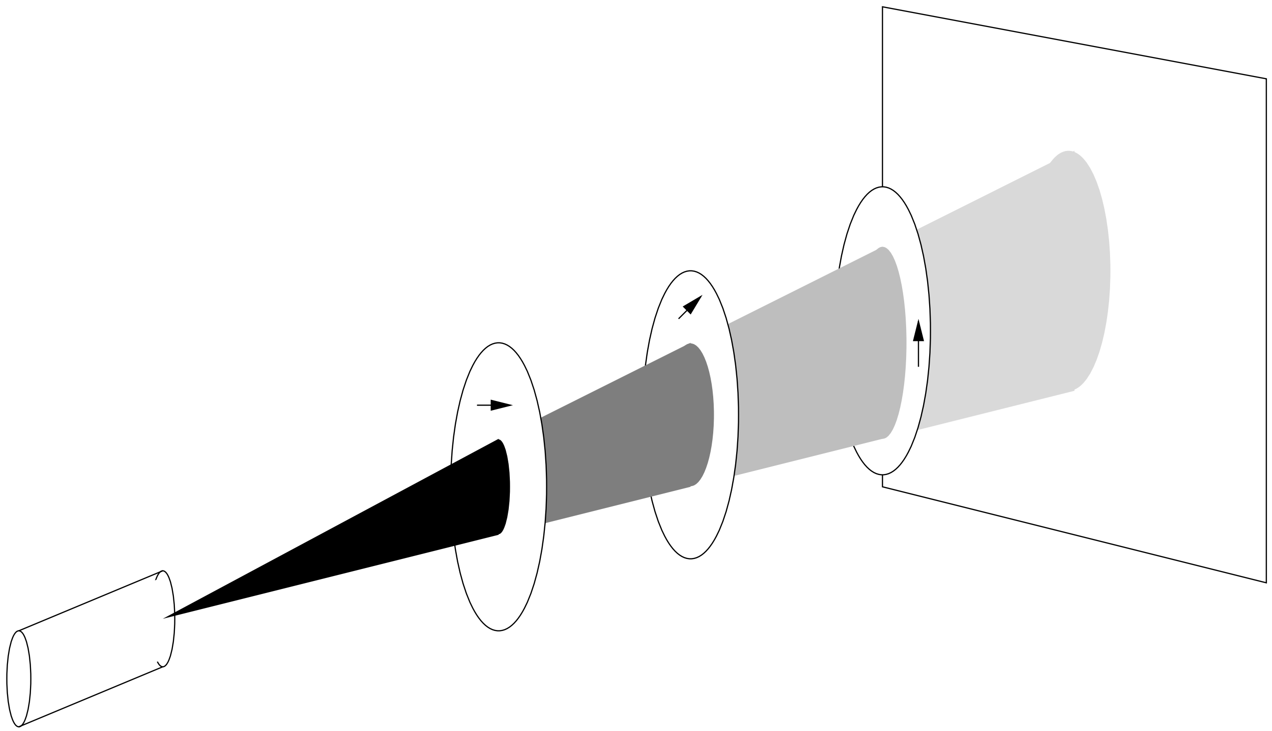
A Simple Experiment: Photon Polarization



A Simple Experiment: Photon Polarization



A Simple Experiment: Photon Polarization



Mathematically Representing Photon Polarization

Polarization state of a photon

- can be represented as a 2-dimensional vector of unit length

Taking horizontal $|{\rightarrow}\rangle$ and vertical $|{\uparrow}\rangle$ polarizations as a basis, an arbitrary polarization can be expressed as a superposition

$$|\psi\rangle = a|{\uparrow}\rangle + b|{\rightarrow}\rangle$$

with $|a|^2 + |b|^2 = 1$

(Allowing a and b to be complex numbers enables this formalism to describe circular polarization as well)

$|v\rangle$ is Dirac's notation for vectors. Means the same thing as $\vec{v}$ or $\mathbf{v}$, with v being the label for the vector

Measurement of Polarization

Polarization filters are quantum measuring devices

Quantum measurements always occur w.r.t. an orthogonal subspace decomposition associated with the measuring device

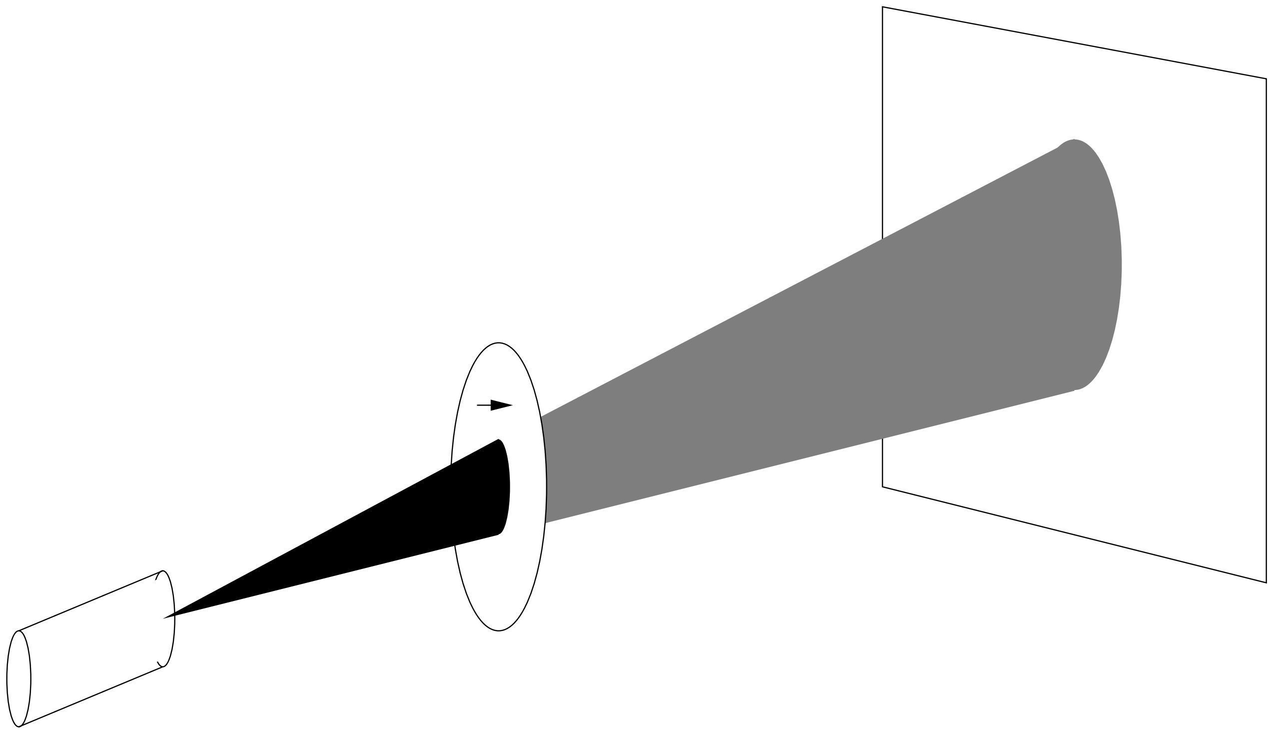
For a horizontal polarization filter, the basis in which it measures is $|\rightarrow\rangle$, together with its perpendicular $|\uparrow\rangle$

A photon with polarization $a|\uparrow\rangle + b|\rightarrow\rangle$ is measured by a horizontal filter as $|\uparrow\rangle$ (absorbed) with probability $|a|^2$, and
$|\rightarrow\rangle$ (passed) with probability $|b|^2$

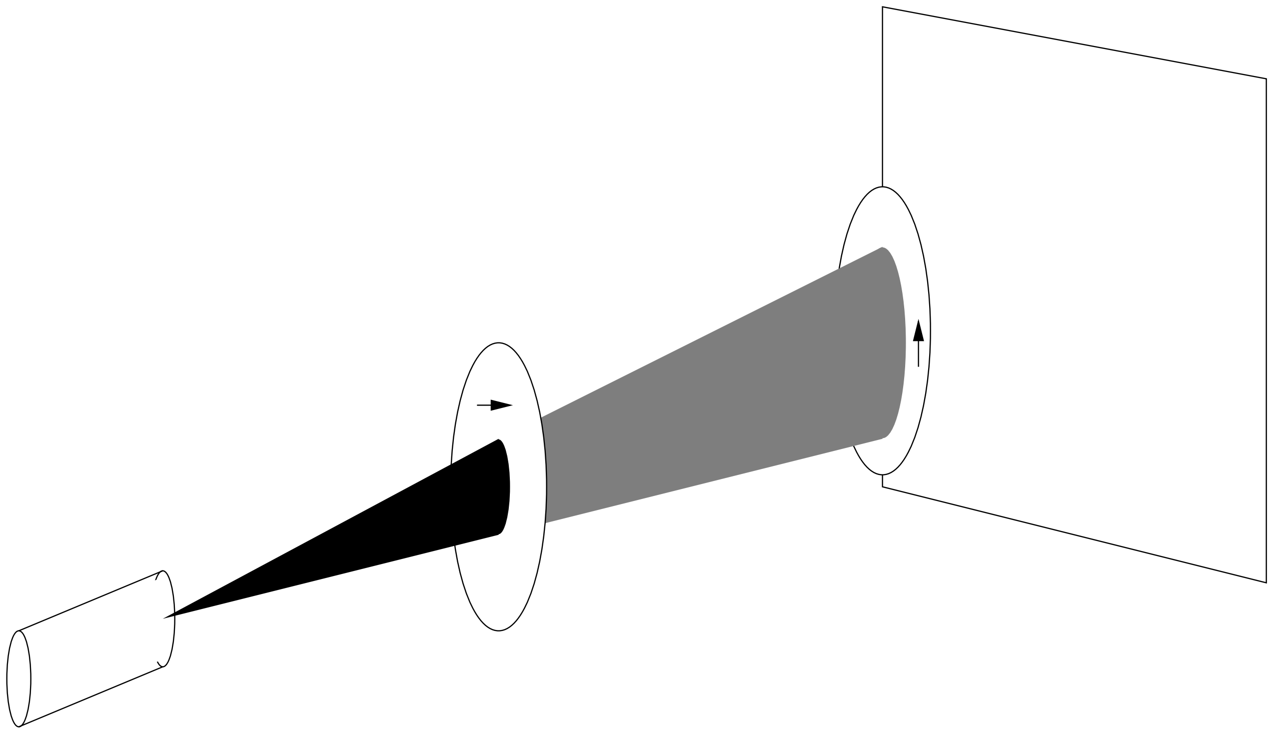
Any photon that has passed through the filter now has polarization $|\rightarrow\rangle$.

Polarization filters at other angles work in a similar way

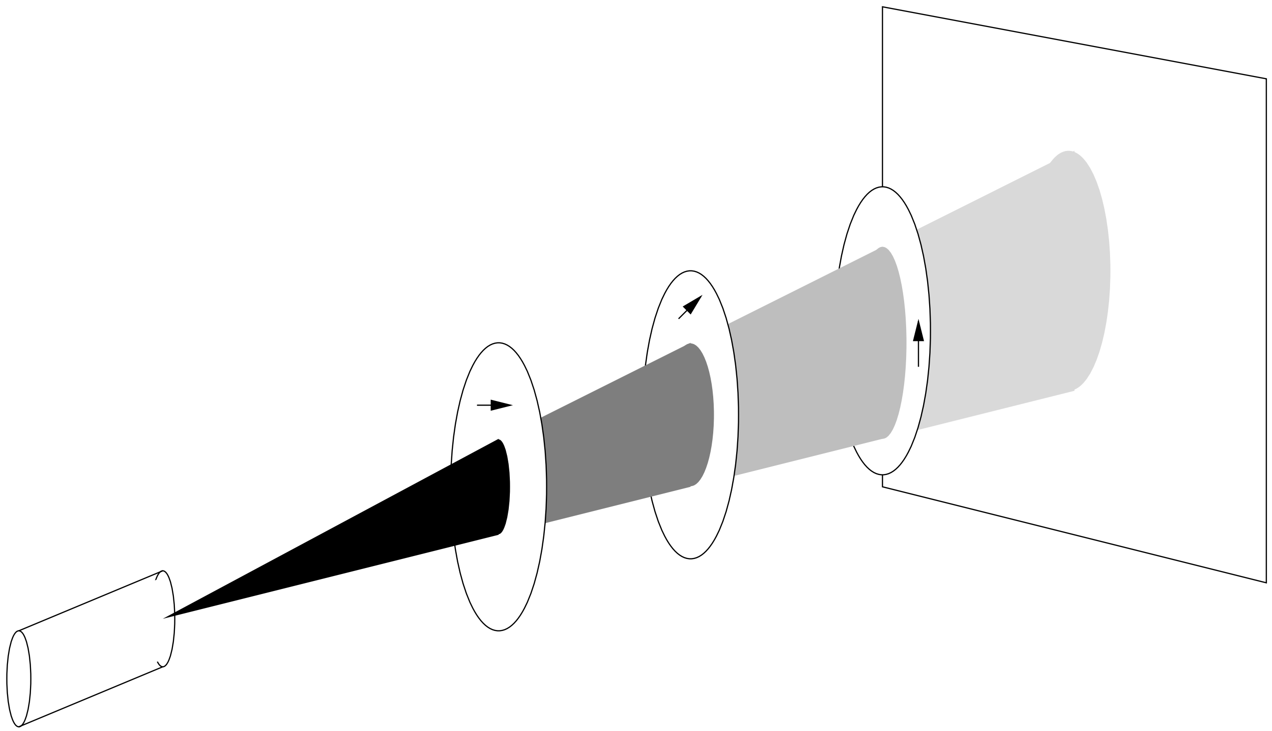
A Simple Experiment: Photon Polarization



A Simple Experiment: Photon Polarization



A Simple Experiment: Photon Polarization



Qubits (Quantum Bits)

Think polarization states of a photon!

Any 2-dimensional quantum system can be viewed as the fundamental unit of quantum computation, a *quantum bit* or *qubit*.
Qubit state space is a 2-dimensional complex vector space

A computational basis is chosen, denoted $|0\rangle$ and $|1\rangle$, and used to encode classical bit values 0 and 1

Possible qubit values $a|0\rangle + b|1\rangle$, for complex a, b with $|a|^2 + |b|^2 = 1$.

Unlike classical bits, qubits can be in superposition states such as $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Measurement of Single Qubits

Measuring qubit $a|0\rangle + b|1\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$

- returns 0 with probability $|a|^2$
- returns 1 with probability $|b|^2$
- projects to state to the basis state corresponding to the measurement result

A qubit can be measured with respect to any orthogonal basis for its 2-dimensional state space

Only one classical bit of information can be extracted from one qubit

No cloning theorem: An unknown quantum state cannot be reliably copied

Multiple Qubits

- Qubits combine like quantum particles not classical objects
  - Quantum states combine via tensor products not direct products
  - The quantum state space, the space of possible states of n quantum particles, is exponentially larger than that of n classical objects
  - 2^n instead of $2n$
- Entangled states make up the bulk of this space
- No classical analog: The state of entangled multiple particle systems cannot be described in terms of the states of the individual particles

High-level View of How State Spaces Combine

Let X be a vector space with basis $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle\}$ and Y be a vector space with basis $\{|\beta_1\rangle, \ldots, |\beta_m\rangle\}$

Classical state spaces combine via the **Cartesian product**

$X \times Y$ has basis $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle, |\beta_1\rangle, \ldots, |\beta_m\rangle\}$

$$\begin{aligned} \dim(X \times Y) &= \dim(X) + \dim(Y) \\ &= n + m \end{aligned}$$

Quantum state spaces combine via the **tensor product**

$X \otimes Y$ has basis $\{|\alpha_1\rangle \otimes |\beta_1\rangle, |\alpha_1\rangle \otimes |\beta_2\rangle, \ldots, |\alpha_n\rangle \otimes |\beta_m\rangle\}$

$$\begin{aligned} \dim(X \otimes Y) &= \dim(X) * \dim(Y) \\ &= n * m \end{aligned}$$

Exponential State Space

The quantum state of an n qubit system is a vector in a 2^n-dimensional space

If B is the state space of a single qubit spanned by $\{|0\rangle, |1\rangle\}$, then a 2-qubit system $B \otimes B$ has basis

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\},$$

often written

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\},$$

The standard computational basis for the 2^n-dimensional complex vector space $B \otimes B \dots B \otimes B$ of an n qubit system is

$$\{|00\dots00\rangle, |00\dots01\rangle, \dots, |11\dots10\rangle, |11\dots11\rangle\}$$

We'll use the notation $|5\rangle = |101\rangle$ when n is understood.

Quantum vs. classical state spaces

A general n-qubit state can be written as

$$\sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

where $\sum_i |\alpha_i|^2 = 1$

Since $2n \ll 2^n$, most n-qubit states cannot be described by the states of the individual qubits

- Most states **cannot** be written as the tensor product of individual qubit states
- (All states can be written as a linear combination of such states.)

States that cannot be written as the tensor product of individual qubit states are called *entangled* states

- These states have no classical counterpart

Measurement in multiqubit systems

Any measuring device has an associated splitting of the 2^n–dim state space $\mathcal{H}$ into orthogonal subspaces $S_1, \ldots, S_k$ with $\mathcal{H} = S_1 \times S_2 \times \cdots \times S_k$

- The only possible outcomes of a measurement are states in one of the subspaces of the orthogonal decomposition associated with the device

Measurement is probabilistic

- Depends on the amplitude of the state in each subspace
- When the device measures a quantum state $|\psi\rangle$, one of the S_j's is chosen with probability the square of the amplitude of the component of $|\psi\rangle$ in S_j

Measurement changes the state

- To one compatible with the measurement result (in the right subspace).
- The state after measurement is the unit vector aligned with the projection of the original state onto S_j

Entangled States

Entangled states cannot be written as tensor product of independent qubits

Example: An EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

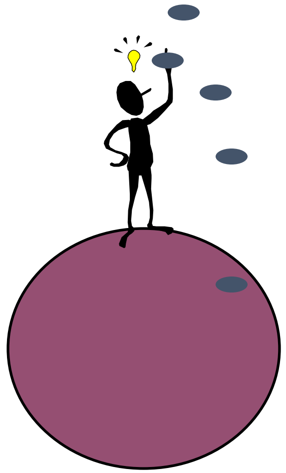
$$\begin{aligned} & (a_0|0\rangle + b_0|1\rangle) \otimes (a_1|0\rangle + b_1|1\rangle) \\ = \quad & a_0 a_1|00\rangle + a_0 b_1|01\rangle + b_0 a_1|10\rangle + b_0 b_1|11\rangle \\ \neq \quad & a_0 a_1|00\rangle + 0|01\rangle + 0|10\rangle + b_0 b_1|11\rangle \\ = \quad & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned}$$

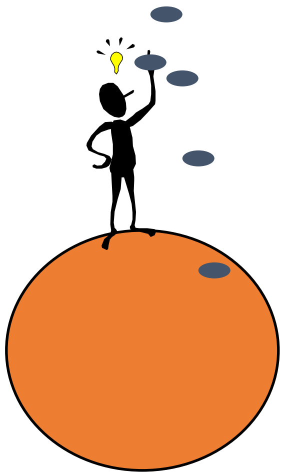
- Measurement of the first qubit yields either $|0\rangle$ or $|1\rangle$
- Measurement changes state to either $|00\rangle$ or $|11\rangle$
- Measurement of second qubit gives same result as first

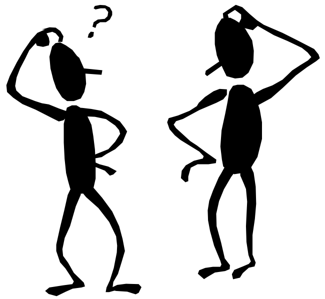
Similar results when measuring in other bases

Entanglement, correlations, and communication

- Two people each see completely random results from their coin tosses
- Completely correlated results!
  - But no way to know this unless they communicate
- There is no way to use this to communicate
  - Different relativistic frames disagree about who flipped the coin first







Critically important also: the behavior when they measure in different basis.

Three paradigms for quantum computing

Quantum circuit model

- Start in a known quantum state (incl. input data)
- Apply a sequence of 1 or 2 qubit quantum logic gates
- Measure to obtain final answer

Adiabatic quantum computation

- Define a final Hamiltonian Hf whose ground state is the solution to the computational problem under consideration
- Start in the ground state of an easily implementable Hamiltonian H0 Evolve the system slowly along a path between H_0 and H_f
- Measure to obtain final answer

Measurement-based quantum computation

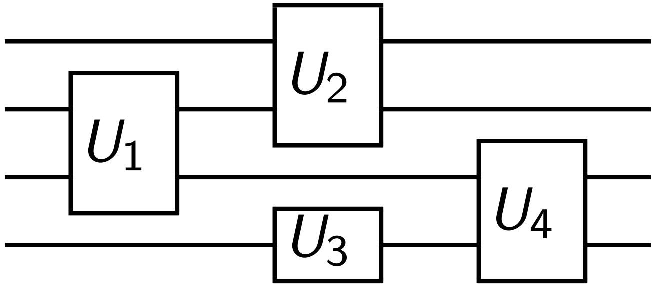
- Start in a highly entangled state that serves as the quantum resource
- Make a series of single qubit measurements that depend on the results of previous measurements
- Interpret the results of the measurements to obtain a final answer

Quantum Computer (Circuit Model)

A quantum computation consists of

- initialization of n-qubit register ($|\psi\rangle$)
- quantum state transformation of register
    - sequence of primitive (1- or 2-qubit) operations (gates) U_i that collectively perform the transformation of the register
- measurement of some or all of the qubits of the register
- classical control throughout to
    - program which quantum steps to carry out
    - interpret results of quantum measurement

$$(I \otimes I \otimes U_4)(U_2 \otimes I \otimes U_3)(I \otimes U_1 \otimes I)|\psi\rangle$$



Some single qubit quantum gates

$$
\begin{array}{rlcll}
I: & |0\rangle & \rightarrow & |0\rangle & \text{Identity} \\
 & |1\rangle & \rightarrow & |1\rangle & \\
X: & |0\rangle & \rightarrow & |1\rangle & \text{Negation, } XX = I \\
 & |1\rangle & \rightarrow & |0\rangle & \\
T(\alpha): & |0\rangle & \rightarrow & e^{\mathbf{i}\alpha}|0\rangle & \text{Variable phase shift} \\
 & |1\rangle & \rightarrow & e^{-\mathbf{i}\alpha}|1\rangle & \\
Y: & |0\rangle & \rightarrow & -1|1\rangle & \text{Negation \& phase shift} \\
 & |1\rangle & \rightarrow & |0\rangle & \\
H: & |0\rangle & \rightarrow & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{Change of basis, } HH = I \\
 & |1\rangle & \rightarrow & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &
\end{array}
$$

Hadamard basis:

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

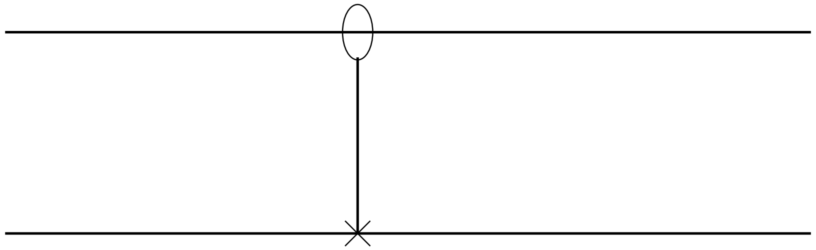
|1> = $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$(H \otimes H \otimes \cdots \otimes H)|00\ldots0\rangle = \frac{1}{\sqrt{2^n}}\sum_i |i\rangle$$

Note: there are infinitely many single qubit gates (e.g. $\alpha \in [0..2\pi]$).

A Multi-qubit quantum gate

Controlled-NOT



$$
\begin{aligned}
C_{not} : \quad |00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |11\rangle \\
|11\rangle &\rightarrow |10\rangle
\end{aligned}
$$

The Controlled-NOT, together with all single qubit gates, is universal for quantum computation.

Observation:

- all quantum gates are linear (actually unitary)
- quantum computations are reversible
- quantum gates do not dissipate energy

> Exercise:
> What does the C_{NOT} do in the Hadamard basis?

Quantum parallelism

By linearity, a superposition of inputs leads to a superposition of results

An quantum circuit can be applied to (a superposition of) all 2^n possible input values at the same time

To obtain the superposition of all values from 0 to $2^n - 1$:

$$\begin{aligned} H \otimes H \otimes \cdots \otimes H|00\ldots0\rangle \quad &\mapsto c(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) \\ &= c \sum |x\rangle \end{aligned}$$

For any sufficiently uniformly computable classical function f, there is a quantum circuit U_f that computes the output in superposition in time comparable to the computation of a single value of a classical function

$$U_f : |x, 0\rangle \to |x, f(x)\rangle$$

$$U_f : c \sum |x_i, 0\rangle \to c \sum |x_i, f(x_i)\rangle$$

A useless example of quantum parallelism

Superposition of inputs leads to superposition of results

Consider $U_\wedge : |x, y, 0\rangle \rightarrow |x, y, x \wedge y\rangle$:

Input	Output
$\|x\rangle \otimes \|y\rangle \otimes \|0\rangle$	$\|x\rangle \otimes \|y\rangle \otimes \|x \wedge y\rangle$
$\frac{1}{2}(\quad \|000\rangle$	$\frac{1}{2}(\quad \|000\rangle$
$+ \quad \|010\rangle$	$+ \quad \|010\rangle$
$+ \quad \|100\rangle$	$+ \quad \|100\rangle$
$+ \quad \|110\rangle)$	$+ \quad \|111\rangle)$

The input and the output, the values of x, y, and $x \wedge y$, are now entangled

Measuring the output in the standard basis randomly yields one line of the truth table

A useful example of quantum parallelism

Quantum Fourier transform:
Let $F\vec{a}$ be the Fourier transform of $\vec{a}$. There is an efficient quantum algorithm Q such that:

$$Q\left(\sum a_i|i\rangle\right) = \sum (F\vec{a})_j|j\rangle.$$

If U_f is a quantum algorithm that computes a periodic function f then

$$U_f(c\sum|i\rangle|0\rangle) = c\sum|i\rangle|f(i)\rangle$$

Measuring the second part $(f(i))$ of the register yields a random value x and collapses the state to

$$\sum a_i|i\rangle|x\rangle = |\psi\rangle \otimes |x\rangle$$

where $a_i \neq 0$ if and only if $f(i) = x$. Then

$$Q|\psi\rangle = \sum (F\vec{a})_j|j\rangle$$

where $(F\vec{a})_j \neq 0$ if j is a multiple of the frequency of f
The period of f can be computed classically from a measurement of j

Shor's algorithm in one slide

Elementary number theory: to factor M it suffices to find the period of function $f(x) = a^x \bmod M$ for some random a, $0 < a < M$

Compute f for all 2^n values simultaneously using quantum parallelism

Apply a quantum Fourier transform (QFT) to get only multiples of the inverse of the period, $k\frac{1}{P}$

Measure. Take denominator as guess for period. We get the right answer when k and P are relatively prime

This algorithm succeeds with high probability. Repeat if it fails.

Brief glimpse of further topics

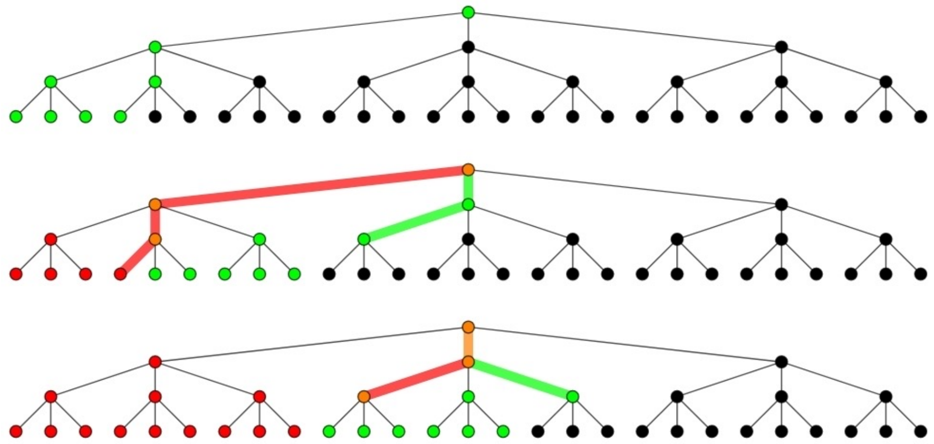
Brief Glimpse: Quantum-accelerated Constraint Programming

In constraint programming (CP), problems are solved with backtracking tree search augmented by logical inference

Quantum algorithms can accelerate the inference process being performed at each node in the tree

These quantum inference algorithms can then be integrated within classical, fully-quantum, or partially-quantum backtracking tree search schemes

Partially quantum backtracking schemes yield speedups for smaller sections of the tree, intended for early, more resource-constrained quantum devices



Other good target state-of-the-art classical algorithms for quantum acceleration?

Booth, Kyle EC, Bryan O'Gorman, Jeffrey Marshall, Stuart Hadfield, and Eleanor Rieffel. **Quantum-accelerated global constraint filtering.** In *International Conference on Principles and Practice of Constraint Programming*, pp. 72-89. 2020

Booth, Kyle EC, Bryan O'Gorman, Jeffrey Marshall, Stuart Hadfield, and Eleanor Rieffel. **Quantum-accelerated constraint programming**. *Quantum* 5 (2021): 550.

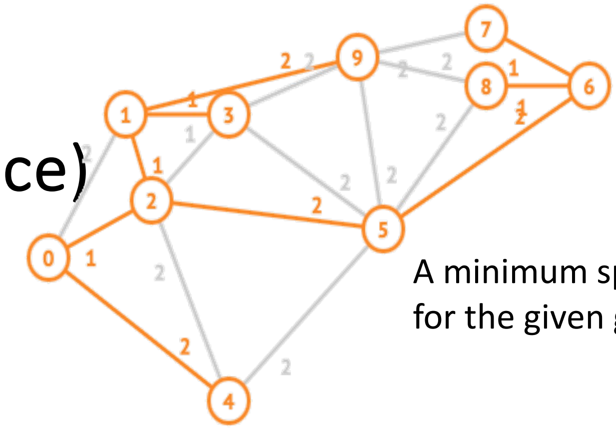
Our Contributions

New algorithms in Quantum CONGEST-CLIQUE Model (qCCM) that succeed with high probability for

- (approximately optimal) Steiner Trees
- Directed Minimum Spanning Trees (Arborescence)

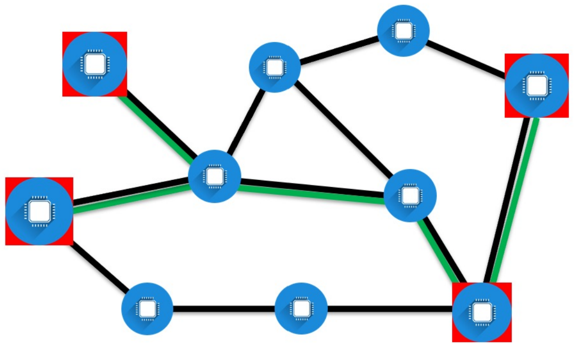
in asymptotically fewer rounds required than for any known classical algorithm

$\rightarrow \tilde{O}(n^{1/4})$ versus $\tilde{O}(n^{1/3})$



A minimum spanning tree (orange) for the given graph (grey)

Exact complexity analysis of quantum and classical algorithms reveals improvements needed for both to become practical! $n > 10^{18}$



Steiner tree (green) for graph with marked terminal nodes (red)

Phillip A. Kerger, David E. Bernal Neira, Zoe Gonzalez Izquierdo, Eleanor G. Rieffel, "Mind the Õ: asymptotically better, but still impractical quantum distribute algorithms," Algorithms 16(7), 332, 2023. *arXiv:2304.02825*

Wigner's friend inequalities & Experiments

Wigner friend scenario recent work

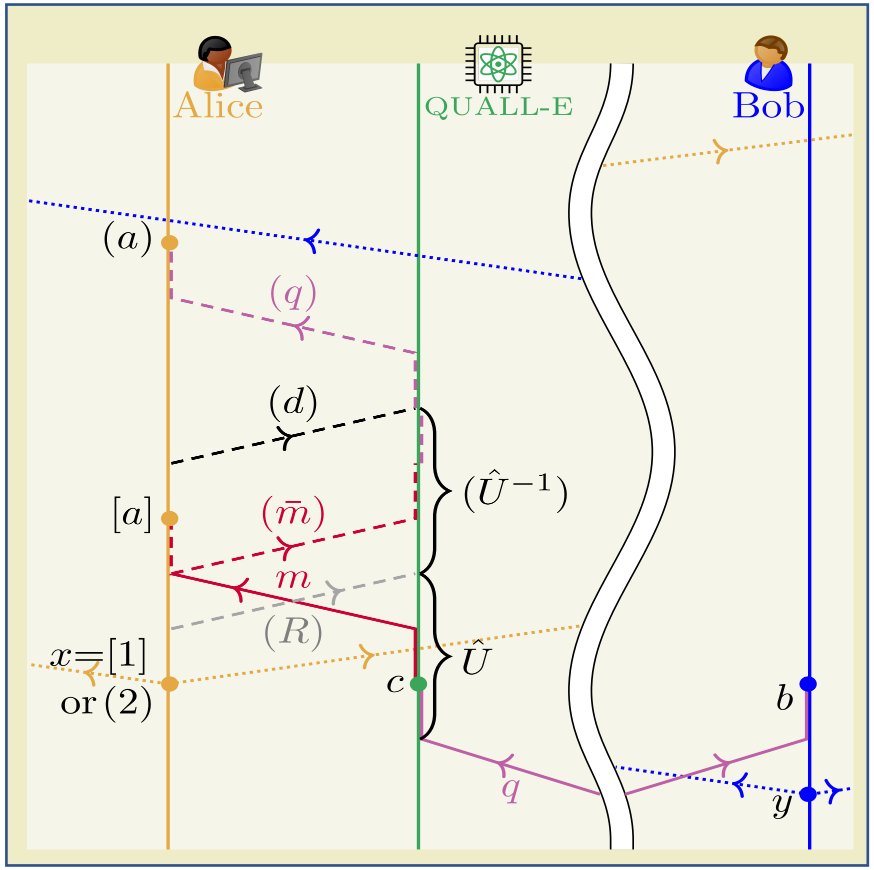
- new inequalities, with weaker assumptions than Bell's inequalities
- Proof-of-principle experiments have been done
  - Single photon as friend

Full experiment would combine Artificial Intelligence and Quantum Computing

- QUALL-E

Open research directions for experiments between proof-of-principle and full

- Space-based experiments



Bong, Kok-Wei, Aníbal Utreras-Alarcón, Farzad Ghafari, Yeong-Cherng Liang, Nora Tischler, Eric G. Cavalcanti, Geoff J. Pryde, and Howard M. Wiseman. **"A strong no-go theorem on the Wigner's friend paradox." Nature Physics 16, 12 (2020)**

H.M. Wiseman, E.G. Cavalcanti, E.G. Rieffel, **A "thoughtful" Local Friendliness no-go theorem: a prospective experiment with new assumptions to suit**, *arXiv:2209.08491 (Accepted to Quantum)*

PySA: Suite of physics inspired classical optimization algorithms

Features and state-of-the-art implementations:

- Modern C++17 with template metaprogramming for high level of abstraction
- Compile time optimization for improved performance

Algorithms:

- Parallel Tempering
- Ergodic and non-ergodic Isoenergetic cluster moves
- Approximate solution using mean-field theory

Recent augmentations:

- Improved Python interface

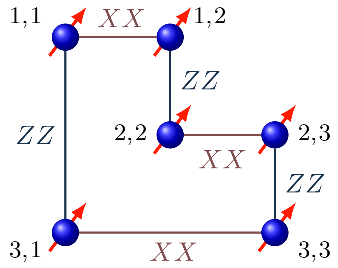
We continuously update PySA with optimized code for state-of-the-art classical optimization, including physics inspired approaches we have developed

Open Source Code: https://github.com/nasa/pysa

Quantum Error Correction

Error suppression: Inhibits transitions out of the desired subspace

Error correction: Corrects errors that have happened



Quantum error correction initially thought impossible!

- No cloning principle: an unknown quantum state cannot be copied reliably without destroying the original

Quantum information theory was just too interesting

- Steane and Shor & Calderbank saw a way to finesse what had seemed insurmountable barriers to quantum error correction

Now quantum error correction is one of the most developed areas

- beautiful, almost magical, effects!
- uses properties of quantum measurement and entanglement to its advantage

Stabilizer code formulation

Subsystem codes; Dynamical Logical Qubits; LDPC codes; …

Fault Tolerance

Error correction mechanisms cannot be done perfectly

Fault tolerance: Ensures error suppression/correction do not introduce more problems than they solve

Imprecise implementation of mechanisms may cause errors. Even accurate implementation can magnify errors

- can take correctable errors to uncorrectable ones

Threshold theorems: There exists an error rate threshold below which indefinitely long quantum computations can be carried out robustly

In the gate model, a number of different threshold theorems are known. Specific theorems involve precise statements of error model, precision of implementation, resource quantification, distance measure

How to establish a threshold theorem for adiabatic quantum computing remains a major open question

HybridQ: A Hybrid Quantum Simulator for Large Scale Simulations

INTELLIGENT SYSTEMS DIVISION

Hardware agnostic quantum simulator, designed to simulate large scale quantum circuits

Can run tensor contraction simulations, direct evolution simulation and Clifford+T simulations using the same syntax

Features:

- Fully compatible with Python (3.8+)
- Low-level optimization achieved by using C++ and Just-In-Time (JIT) compilation with JAX and Numba,
- It can run seamlessly on CPU/GPU and TPU, either on single or multiple nodes (MPI) for large scale simulations, using the exact same syntax
- User-friendly interface with an advanced language to describe circuits and gates, including tools to manipulate/simplify circuits.

Recent Improvements:

- Commutations rules are used to simplify circuits (useful for QAOA)
- Expansion of density matrices as superpositions of Pauli strings accepts arbitrary non-Clifford gates,
- Open-source project with continuous-integration, multiple tests and easy installation using either `pip` or `conda`

Open source code available at https://github.com/nasa/HybridQ

S. Mandrà, J. Marshall, E. G. Rieffel, R. Biswas, HybridQ: A Hybrid Simulator for Quantum Circuits, QCS 2021, arXiv:2111.06868

NASA Ames director Hans Mark brought the Illiac IV to NASA Ames in 1972

Illiac IV – first massively parallel computer

- 64 64-bit FPUs and a single CPU
- 50 MFLOP peak, fastest computer at the time

Finding good problems and algorithms was challenging

Questions at the time:

- How broad will the application be of massively parallel computing?
- Will computers ever be able to compete with wind tunnels?

Take-away points

If we were handed a robust, scalable quantum quantum computer today, for many problems, we would not know what algorithm to run or if quantum computers can help

Lots of work still to be done on quantum algorithms, both

- Heuristic, and
- Those amenable to analysis and proofs

Exciting times ahead, especially as prototype systems improve

Many opportunities for classical computing to inform quantum computing and to work with or as part of quantum computing

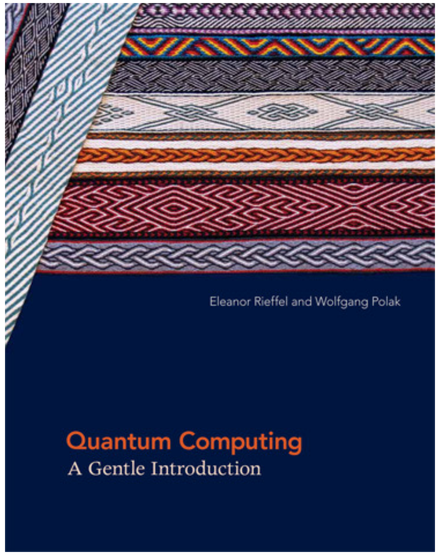
Many examples of quantum computing inspiring better classical algorithms

- Quantum-inspired algorithms
- Quantum-spurred algorithms

Hardware-algorithms codesign will be key to advances in coming years

Enjoy learning more about this fascinating field!

Further Reading



Eleanor Rieffel and Wolfgang Polak
Quantum Computing: A Gentle Introduction
MIT Press, March 2011

And references therein

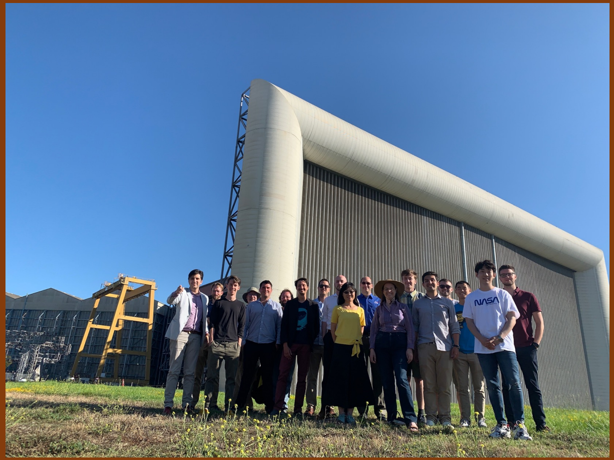
Overviews of NASA QuAIL team work

Eleanor G. Rieffel, Stuart Hadfield, Tad Hogg, Salvatore Mandrà, Jeffrey Marshall, Gianni Mossi, Bryan O'Gorman, Eugeniu Plamadeala, Norm M. Tubman, Davide Venturelli, Walter Vinci, Zhihui Wang, Max Wilson, Filip Wudarski, Rupak Biswas, ***From Ansätze to Z-gates: a NASA View of Quantum Computing***, arXiv:1905.02860

Rupak Biswas, Zhang Jiang, Kostya Kechezhi, Sergey Knysh, Salvatore Mandrà, Bryan O'Gorman, Alejandro Perdomo-Ortiz, Andre Petukhov, John Realpe-Gómez, Eleanor Rieffel, Davide Venturelli, Fedir Vasko, Zhihui Wang, ***A NASA Perspective on Quantum Computing: Opportunities and Challenges***, arXiv:1704.04836

QuAIL Team

With many thanks to everyone on the NASA QuAIL team!



Lead: Eleanor Rieffel, Deputy Lead: Shon Grabbe, Sohaib Alam, Namit Anand, David Bernal Neira, Jacob Biamonte, Lucas Brady, Stephen Cotton, Zoe Gonzalez Izquierdo, Erik Gustafson, Stuart Hadfield, Aaron Lott, Salvatore Mandrà, Filip Maciejewski Jeffrey Marshall, Gianni Mossi, Jason Saied, Nischay Suri, Norm Tubman, Davide Venturelli, Zhihui Wang