Iowa State University

Department of Physics and Astronomy

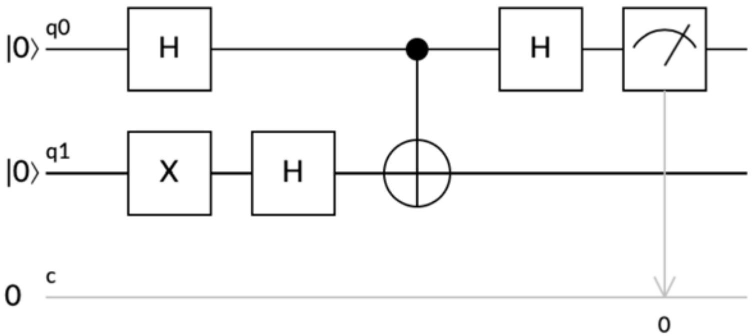
The Future of Computation: Unleashing the Power of Quantum Computers

Peter P. Orth (Iowa State University and Ames Laboratory)

[1] Department of Physics and Astronomy, Iowa State University, Ames, Iowa 50011, USA

[2] Ames Laboratory, Ames, Iowa 50011, USA

Physics Colloquium, Western Illinois University, Macomb, Nov 8, 2019



DOE Ames Lab

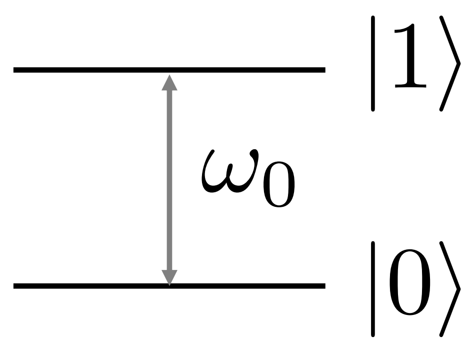
U.S. DEPARTMENT OF ENERGY | Office of Science

What is a quantum computer?

A quantum computer is a programmable computing device that works according to the fundamental physical laws of quantum mechanics.

Properties of a *digital* quantum computer

- Contains qubits (= quantum mechanical two-level systems = spin-1/2)
  - Sounds similar to a classical bit {0, 1}, but is a totally different beast.



What is a quantum computer?

A quantum computer is a programmable computing device that works according to the fundamental physical laws of quantum mechanics.

Properties of a *digital* quantum computer

- Contains qubits (= quantum mechanical two-level systems)
- Quantum gate operations act on qubits and change their states
  - Sounds similar to classical gates {AND, OR, …}, but must be reversible

$$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$$

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

X: flips qubit, acts like NOT gate.

H: generates superposition (Hadamard gate).

What is a quantum computer?

A quantum computer is a programmable computing device that works according to the fundamental physical laws of quantum mechanics.

Properties of a *digital* quantum computer

- Contains qubits (= quantum mechanical two-level systems)
- Quantum gate operations act on qubits and change their state
- Qubits are measured at the end of the computation
  - Quantum state is transformed into classical information
  - Read-out is probabilistic (Born rule)

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Probabilities

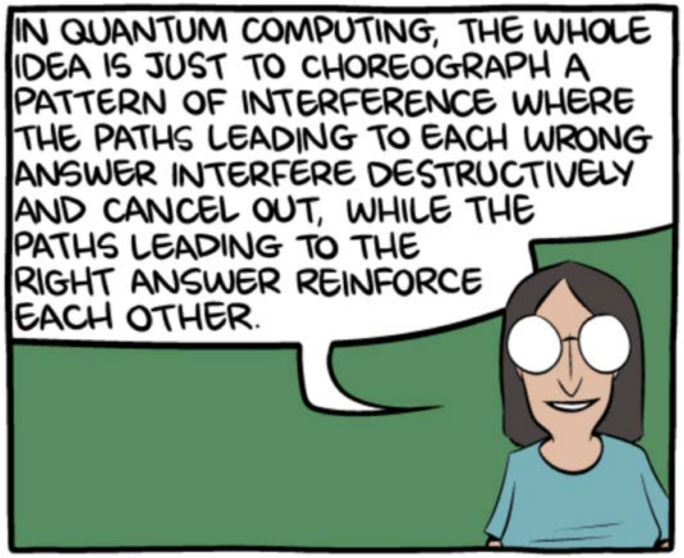
$$|\langle 00|\psi\rangle|^2 = |\langle 11|\psi\rangle|^2 = 1/2$$

$$|\langle 10|\psi\rangle|^2 = |\langle 01|\psi\rangle|^2 = 0$$

What is a quantum computer?

A quantum computer is a programmable computing device that works according to the fundamental physical laws of quantum mechanics.

- Most important differences between classical and quantum computer
  - QC can be in a superposition of bit states
  - QC exhibits interference of different circuit paths, analogous to waves or light
  - QC exhibits entanglement and thus non-local effects
  - QC more powerful for certain tasks (factoring, searching, quantum simulation,..)



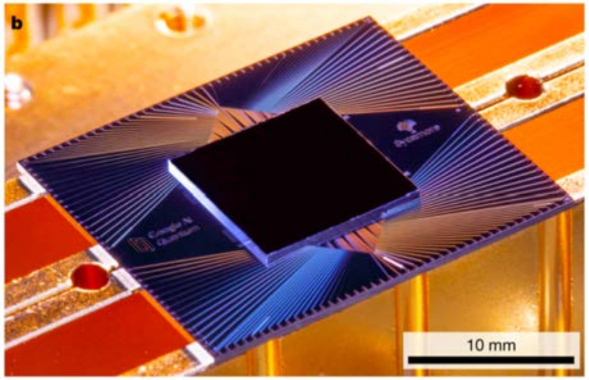
www.scottaaronson.com/blog, smbc-comics.com

How does a quantum computer look like?

Various implementation platforms are being pursued in our quest to build a quantum computer. It is too early to tell which one(s) will succeed.

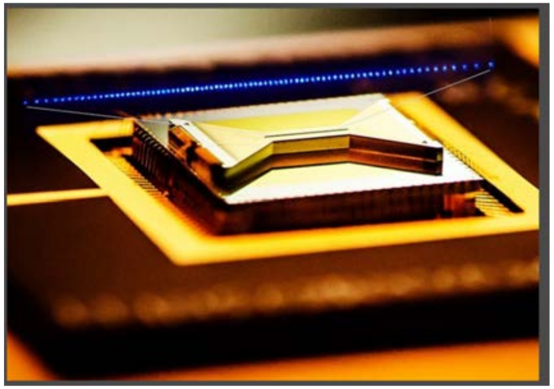
- DiVincenzo criteria
  - Well-characterized qubits, scalability to large systems
  - Ability to initialize state and perform “universal” set of gate operations
  - Long lifetime of quantum state >> gate operation
  - Measurement capability

Superconducting qubits (Yale, UCSB, Zuerich, IBM, Google, Rigetti, …)



J. Martinis *et al.*, Nature **574**, 505 (2019).

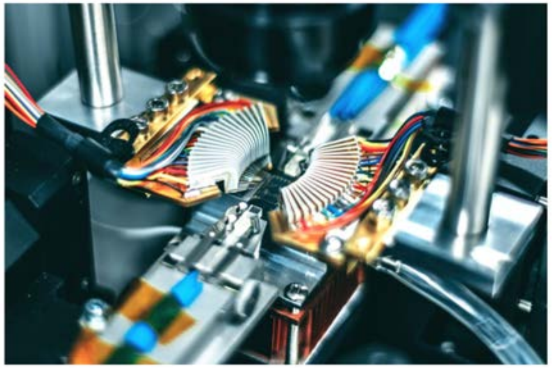
Trapped ions (NIST, Innsbruck, IonQ, Honeywell, Microsoft …)



Taken from website of Chris Monroe (NIST).

Photons (Xanadu, PsiQ, QuiX,…)

& more exist!



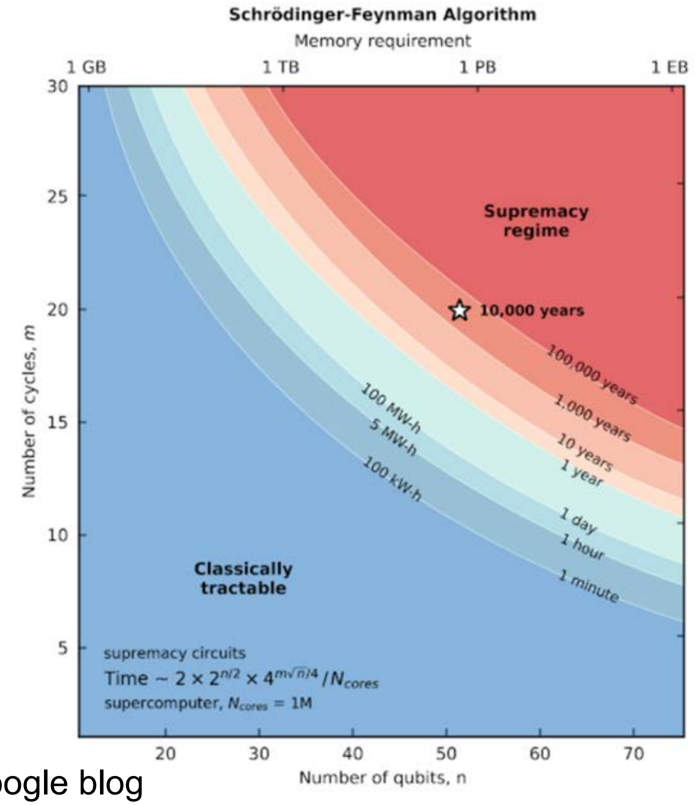
Xanadu chip, taken from Nature website.

What is all the current hype about?

Quantum computing technology is at the beginning of a new era: Noisy Intermediate Scale Quantum (NISQ) computers

- QC devices have now tens of qubits
  - Google Sycamore (53 qubits), IBM Q 53 (53 qubits), Rigetti 19Q Acorn
- Gate fidelity improving to error rates < 1%
- Google announced "quantum supremacy"
  - Definition: "Perform tasks with controlled quantum systems going beyond what can be achieved with ordinary digital computers." (J. Preskill)
  - Performed calculation on "Sycamore" chip in 200 sec that would take 2.5 days on the world's largest supercomputer "Summit" at Oak Ridge National Lab. Google's initial estimate was 10'000 years.

Google's "Sycamore"



From Google blog

Quantum supremacy demonstration

Quantum computing technology is at the beginning of a new era: Noisy Intermediate Scale Quantum (NISQ) computers

- Google's quantum supremacy calculation is important proof-of-principle
- Calculation itself was useless
- Similar to the first airplane flight by the Wright brothers in 1903

Seconds into the first airplane flight, near Kitty Hawk, North Carolina; December 17, 1903, Photo first published in 1908

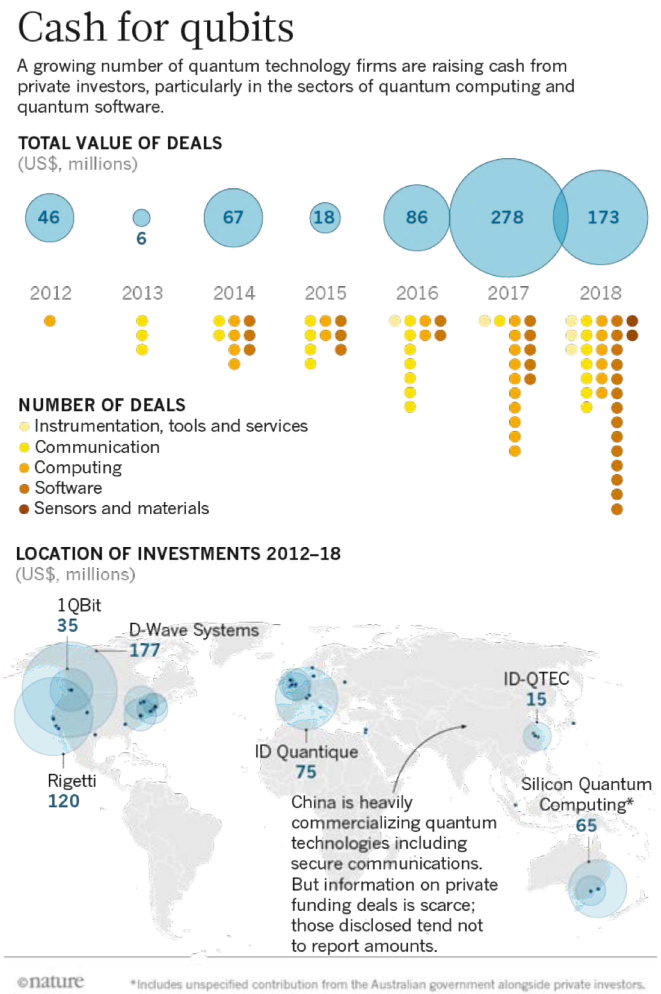
???

Commercial plane

Quantum gold rush

Quantum computing technology is at the beginning of a new era: Noisy Intermediate Scale Quantum (NISQ) computers

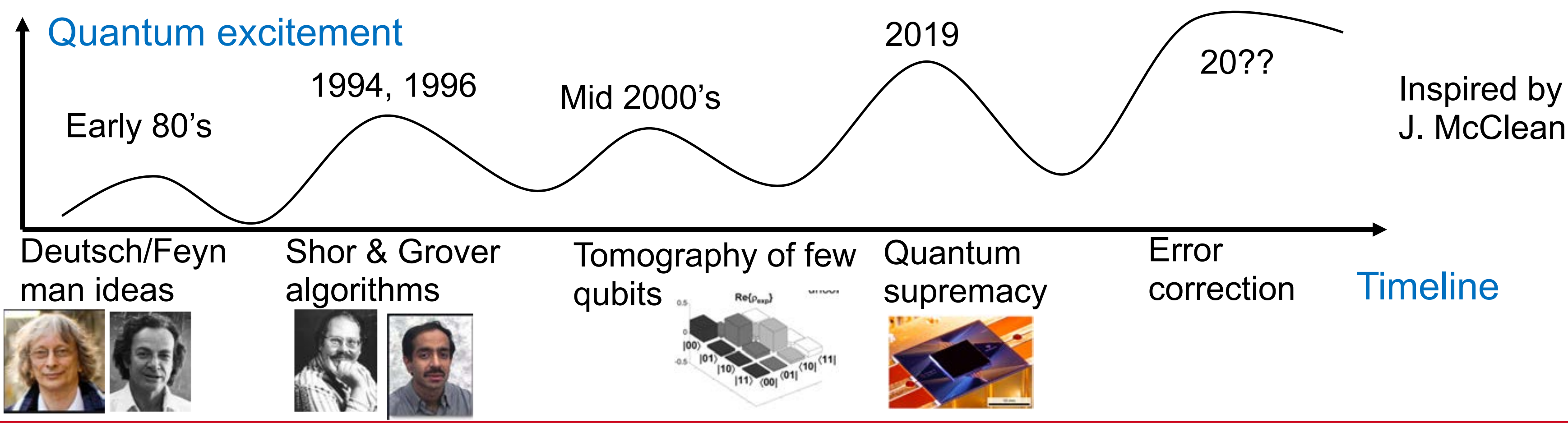
- First useful applications are in sight
  - Quantum chemistry
  - Quantum optimization
  - Hybrid quantum-classical algorithms, e.g., for material science (my work)
  - Machine learning
  - Design of catalysts and drugs
  - Finance
- Quantum gold rush
  - $450M venture capital (VC) invested in 2017/2018
  - Equal to VC for Artificial Intelligence (AI) prior to 2010 (now AI VC = $9.3B)



E. Gibney, Nature **574**, 22 (2019).

Outline

- What is a quantum computer?
  - Qubits, circuits, superposition, interference, entanglement
- What can you do with it?
  - Quantum algorithms, exponential speedup, Hamiltonian simulation
- What is the hype all about?
  - Google's "quantum supremacy" experiment
- What's next?
  - Near-term NISQ applications
  - Roadmap to full fledged quantum computer with error correction



WHAT IS A QUANTUM COMPUTER?

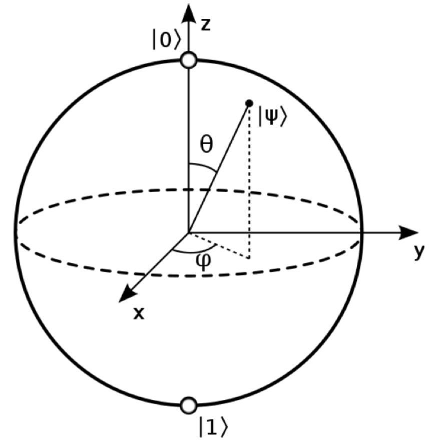
Quantum mechanics 101

- Qubit is a quantum two-level system

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

Superposition

Bloch sphere



- Undergoes unitary evolution following Schrödinger equation

$$\boxed{i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H(t)|\psi(t)\rangle}$$

Unitary = reversible computing

$$U^\dagger = U^{-1}$$

$$\Rightarrow |\psi(t)\rangle = T\exp[-i\int_0^t dsH(s)]|\psi(0)\rangle = U(t)|\psi(0)\rangle$$

Example:

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & e^{i\varphi(t)} \\ 1 & -e^{i\varphi(t)}\end{pmatrix}\begin{pmatrix}1 \\ 0\end{pmatrix}$$

Unitary operator = unitary matrix
multiplying initial state vector $|\psi(0)\rangle = |0\rangle = \begin{pmatrix}1 \\ 0\end{pmatrix}$

Quantum mechanics 101

- Measurement is probabilistic (Born rule)
  - Projection on particular eigenstate |m> of Hermitian operator M (observable)
  - Access only small part of the information contained in quantum state

$$M = \sum_m \lambda_m P_m$$

$$P_m = |m\rangle\langle m|$$

$$\Longrightarrow \boxed{p(m) = \langle\psi|P_m|\psi\rangle}$$

Probability to measure eigenvalue λ_m

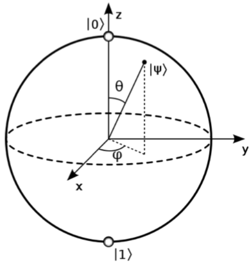
- Example: measurement of observable σ^z

$$P_0 = |0\rangle\langle 0|, P_1 = |1\rangle\langle 1| \Longrightarrow \sigma^z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\lambda_0 = 1, \lambda_1 = -1$$

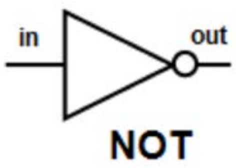
- General wavefunction:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \Longrightarrow \boxed{\begin{aligned} p(0) &= |\langle 0|\psi\rangle|^2 = \cos^2\frac{\theta}{2} \\ p(1) &= |\langle 1|\psi\rangle|^2 = \sin^2\frac{\theta}{2} \end{aligned}}$$

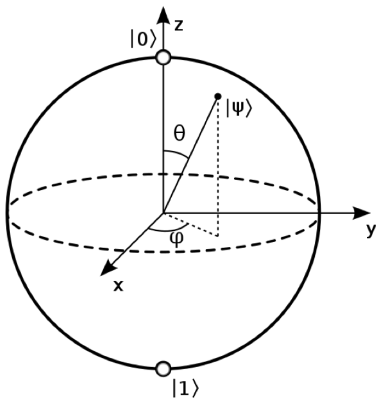


Single qubit quantum gates

- Single-bit gate in classical circuits
  - NOT gate



Input	Output
I	F
0	1
1	0



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

- Unitary single qubit quantum gates
  - X=NOT, Y, Z, phase gate, $\pi/8$, Hadamard gate, general qubit rotation R

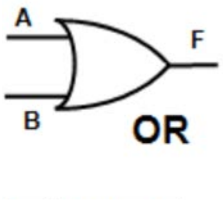
$$X=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Longrightarrow X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$$

$$T=\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \Longrightarrow T|0\rangle = |0\rangle, T|1\rangle = e^{i\pi/4}|1\rangle$$

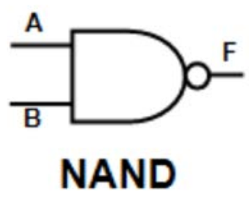
$$H=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \Longrightarrow H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Two and three qubit gates

- Gates in classical circuits
  - OR, NOR, XOR, AND, NAND (some are irreversible like NAND)



Inputs		Output
A	B	F
0	0	0
1	0	1
0	1	1
1	1	1

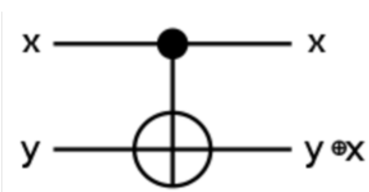


Inputs		Output
A	B	F
0	0	1
1	0	1
0	1	1
1	1	0

NAND gate is universal in classical circuits

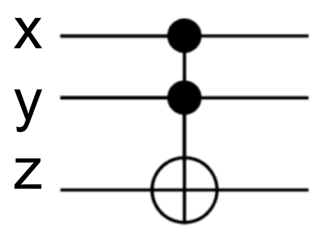
- Two and three qubit quantum gates
  - Controlled-U like CNOT gate creates entanglement between qubits
  - Any multi-qubit gate can be composed of single-qubit and CNOT gates
  - Toffoli three-qubit gate = reversible NAND gate. All classical circuits can be represented as quantum circuit.

CNOT



input		output	
x	y	x	y+x
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Toffoli

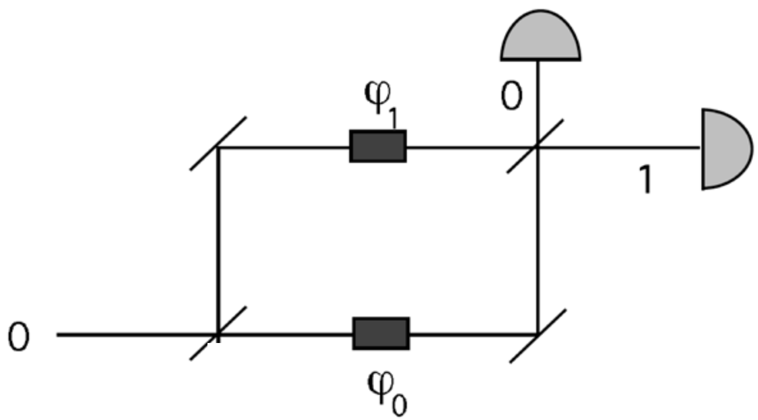


Can represent NAND (z=1) and FANOUT (x=1, z=0) (on basis states)
⇢ classically universal

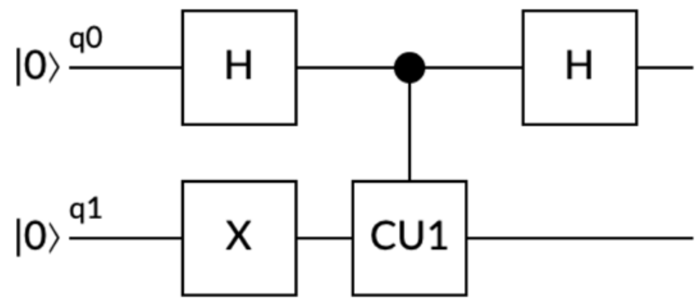
Interference in quantum circuits

- Interference of different circuit paths
  - Outcome depends on phase difference φ along two paths
  - First qubit in state |0> for $\varphi = 0$, and in state |1> for $\varphi = \pi$

Mach-Zehnder light interferometer



Corresponding quantum circuit



$$|00\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)|1\rangle$$

$$\boxed{\to \frac{1}{\sqrt{2}}(\cos\frac{\varphi}{2}|0\rangle - i\sin\frac{\varphi}{2}|1\rangle)|1\rangle}$$

$$\mathrm{CU1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}$$

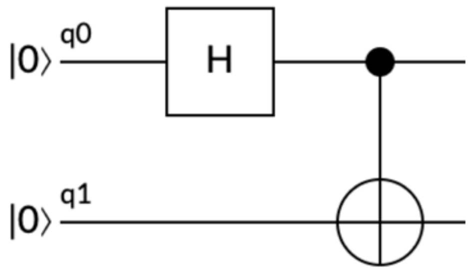
Controlled-U gate

[1] R. Cleve *et al.*, Proc. Soc. Lond. A. (1998)
[2] Figure by C. Addams (NYT)

Entanglement in quantum circuits

- A state that cannot be written as a product state is entangled
  - CNOT gates create entanglement
  - Non-local “correlations” of quantum states (EPR paradox)
  - Can be used for teleportation of a quantum state

Quantum circuit that creates an entangled pair (Bell state)



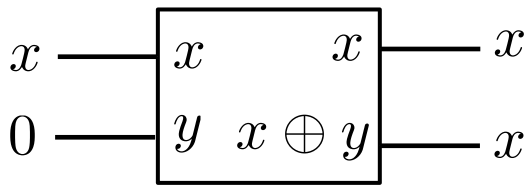
$$|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Cannot be written as $|\psi_1\rangle \otimes |\psi_2\rangle$

- If first qubit is measured to be zero: state of second qubit = |0>
- If first qubit is measured to be one: state of second qubit = |1>
  - Non-local correlations between the two qubits, even if spatially separated!

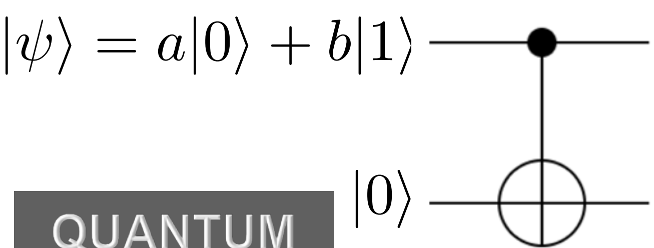
No-cloning theorem

- Classical information can be copied anytime (FANOUT)



Classical CNOT gate copies (unknown) bit x.

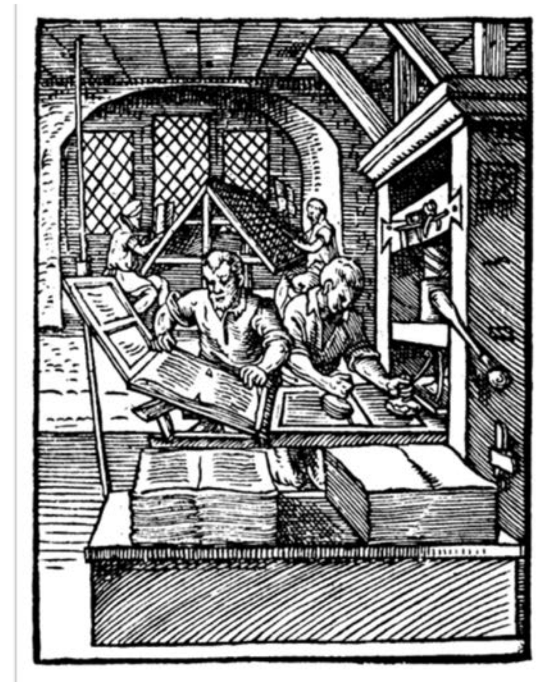
- Cannot copy **unknown** quantum state



$$\boxed{a|00\rangle + b|11\rangle}$$

- Quantum CNOT gate creates entangled state instead

- Otherwise, we would have access to hidden information of quantum state



Early wooden printing press, depicted in 1568. Such presses could produce up to 240 impressions per hour.[16]

Proof of no-cloning theorem

- Imagine quantum machine with two slots A and B
  - Data slot A contains unknown state $|\psi\rangle$
  - Target slot B starts out in some standard pure state $|s\rangle$

$$\boxed{|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle}$$

Ideal situation: unitary U copies state $|\psi\rangle$ into target slot

- Suppose this works for two states:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

$$\boxed{\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2}$$

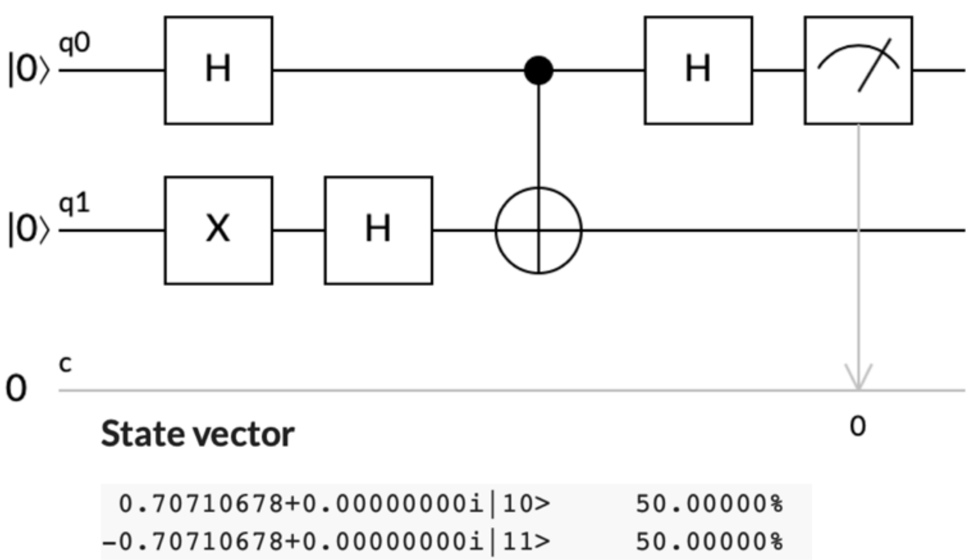
- Only two solutions of $x = x^2 \rightarrow x = 0$ or $x = 1$:

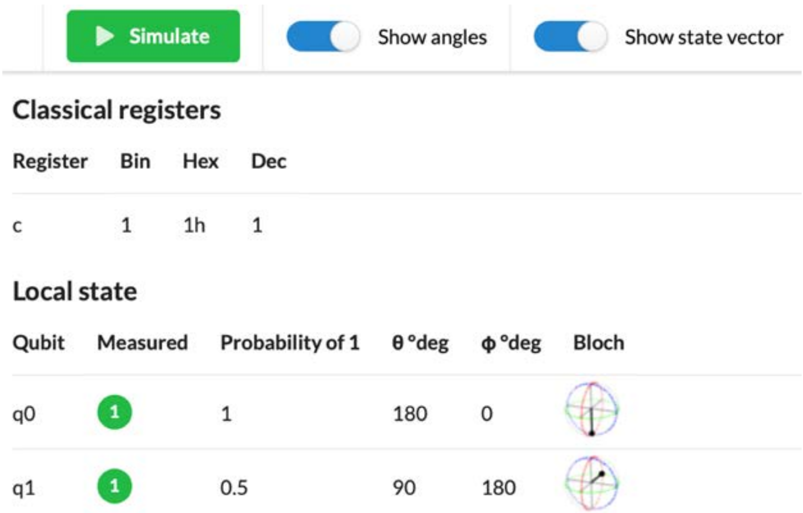
$$x = 0 : |\psi\rangle \perp |\varphi\rangle$$
$$x = 1 : |\psi\rangle = |\varphi\rangle$$

Can only copy the orthogonal (i.e. classical) state. Any other state cannot be cloned.

Implement quantum circuits and run in the cloud

- Different quantum programming frameworks are available
  - QISKIT (IBM): vibrant open source community, many examples
  - Forest, PyQuil (Rigetti): very intuitive syntax, similar to python
  - Circ (Google), Q# (Microsoft), others exist
  - Quantum Programming Studio (QPS): easy drag&drop circuits
- Quantum simulators allow to run circuit on local hardware
  - QISKIT and Rigetti Forest can simulate different noise models
  - QuEST: fastest quantum simulator (open source)





From Quantum Programming Studio

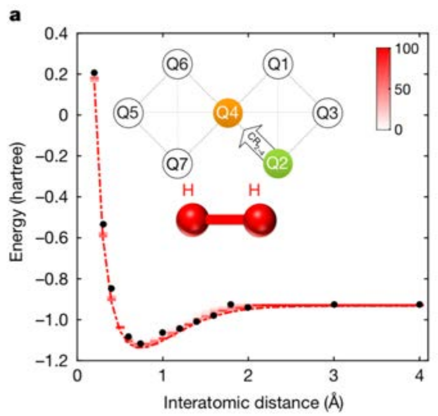
WHAT CAN YOU DO WITH A QUANTUM COMPUTER?

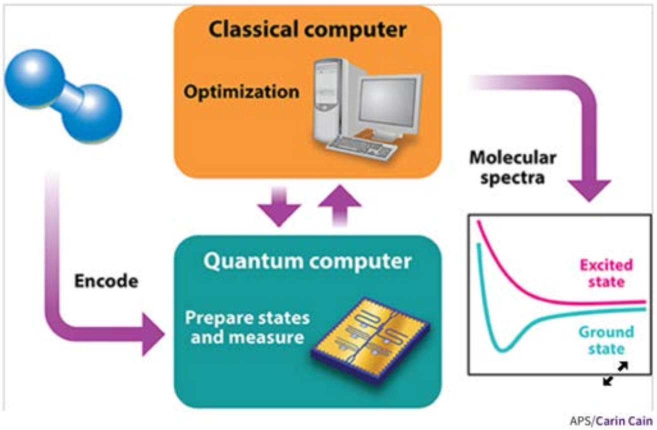
What can you do with a quantum computer?

Quantum computers promise dramatic (exponential) speedups over classical computers for certain tasks. New computing paradigm!

Near term applications:

- Generate truly random numbers
- Simulating quantum physics & chemistry
  - Hilbert space grows exponentially: $N = 2^n$ basis states for n qubits.
  - $N = 10^{16}$ =1000 TB to store wavefunction for $n = 53$ qubits!
  - Idea: prepare state on the QC and measure its properties
- Hybrid quantum-classical algorithms
- Learn new fundamental physics: more is different!





[1] Kandala et al (IBM), Nature (2017); [2] Sim, Alán Aspuru-Guzik et al., Physics Viewpoint (2018).

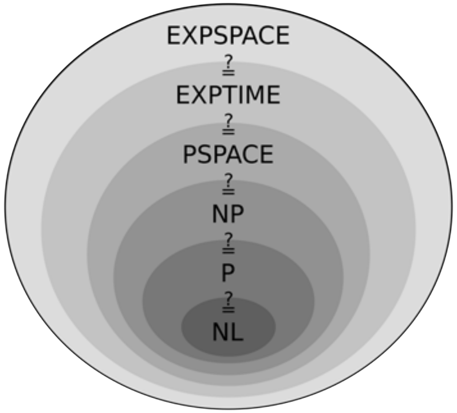
What can you do with a quantum computer?

Quantum computers promise dramatic (exponential) speedups over classical computers for certain tasks. New computing paradigm!

Longer term applications:

- Factor integers (break public-key RSA encryption): Shor algorithm
- Speed up searches of unstructured databases: Grover algorithm
- Prove theorems in complexity theory: $P \neq PSPACE$
- Potentially many more applications!

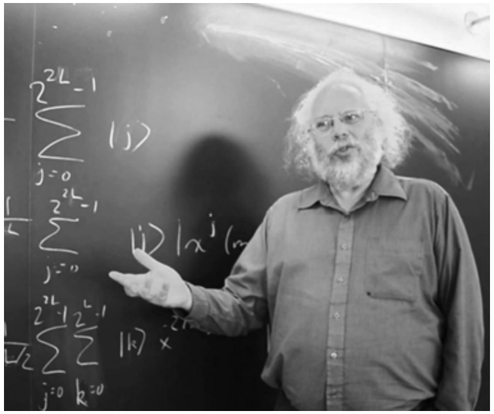
Complexity classes



From Wikipedia

Disney's "Beagle Boys"

Codebreaking is a lot faster with this one..



Peter Shor, taken from dotquantum.io

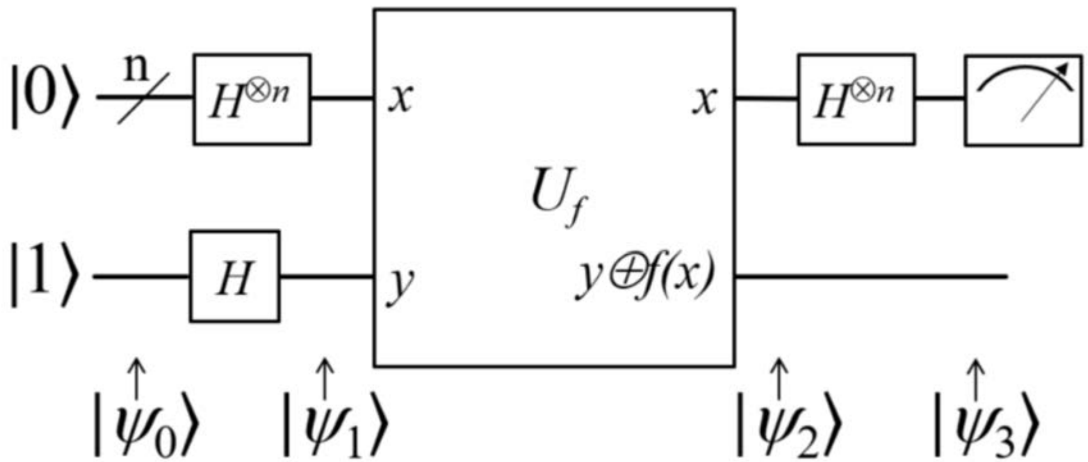
First quantum algorithm: Deutsch-Josza algorithm

Task: A black box U_f performs transformation $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ with $x \in \{0,1\}^n$ and $f(x) \in \{0,1\}$.
It is promised that $f(x)$ is either *constant* or *balanced* (= 1 for exactly half of all possible x and = 0 for the other half).

- Classically, need $N = 2^{n-1} + 1$ function calls in worst case
- Quantum, only one function call needed!
- Exponential speedup!

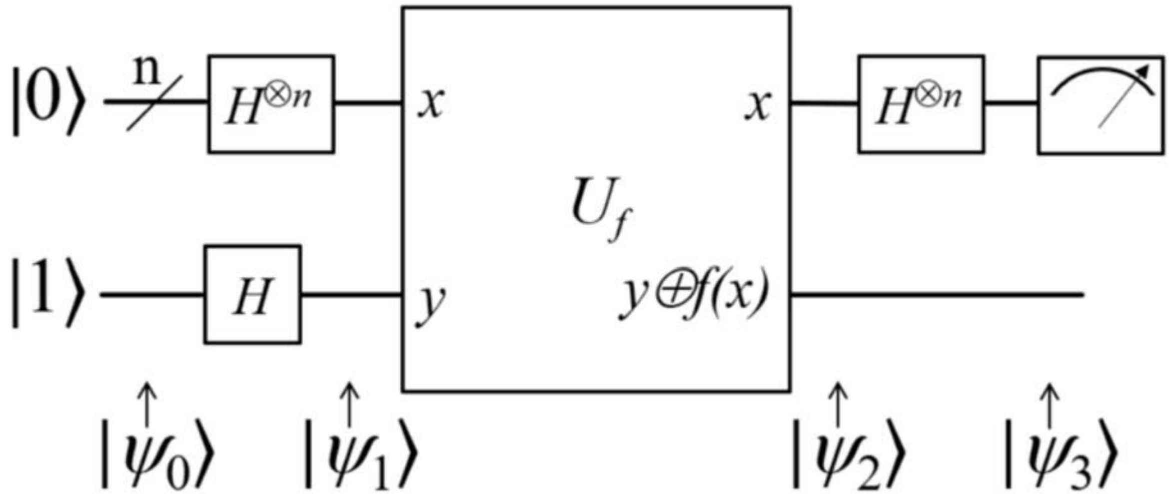
David Deutsch

Richard Josza



Deutsch-Josza quantum circuit (1992)

Deutsch-Josza quantum algorithm



Example for n=1:

$$|\psi_0\rangle = |01\rangle \longrightarrow |\psi_1\rangle = \frac{1}{2}\Big[|0\rangle + |1\rangle\Big]\Big[|0\rangle - |1\rangle\Big]$$

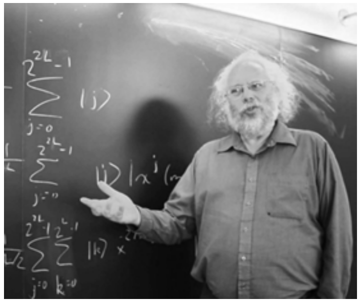
$$|\psi_2\rangle = \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) = \begin{cases} \pm\frac{1}{2}\Big(|0\rangle \boxed{+} |1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) & \text{if } f(0) = f(1) \\ \pm\frac{1}{2}\Big(|0\rangle \boxed{-} |1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) & \text{if } f(0) \neq f(1) \end{cases}$$

$$\boxed{|\psi_3\rangle = \begin{cases} \pm|0\rangle\Big(|0\rangle - |1\rangle\Big) & \text{if } f(0) = f(1) \\ \pm|1\rangle\Big(|0\rangle - |1\rangle\Big) & \text{if } f(0) \neq f(1) \end{cases}}$$

One function call instead of two.
For n qubits: one call instead of $2^{n-1} + 1$ (exponential speedup).

Other quantum algorithms

- Shor algorithm for factorization of integer N=pq into prime factors
  - Exponential speedup: $\mathcal{O}[(\ln N)^2]$ instead of $\mathcal{O}[\exp[2(\ln N)^{\frac{1}{3}}]]$
  - Factorization (probably) not in P, but not NP-complete
  - Examples:
    - 15 = 3 x 5
    - 9999999942014077477 = 3162277633 x 3162277669
  - Would break RSA public-key cryptosystem
  - Requires QC with error correction (decades away)



Peter Shor

Secret message: “Hello Jessica, you have a cool hat!”

Encryption using public key

Jessica’s public RSA key: integers: (n, r)

Message can be sent publicly: “Uryyb Wrffvpn, lbh unir n pbby ung!”

Decryption using private key

Jessica’s private key: (p, q) with $pq = n$

Jessica: “Thank you, Sharky!”

Simulating nature using QC

- R. Feynman: "Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical."
- Hilbert space grows exponentially with the number of particles $N = 2^n$
  - $n = 1000 \to N = 10^{300} \gg 10^{80}$ = number of baryons in the universe
- Cannot even store wavefunction, but QC can create it!

Idea: Prepare wavefunction using gates and measure its properties.

- Common task in physics: find ground state $|\psi_0\rangle$ and GS energy of an interacting Hamiltonian H
- Algorithm: Prepare non-interacting initial state and slowly turn on interactions

$$H(t) = H_0 + tH_{\text{int}}, 0 \leq t \leq 1$$

- Problem: requires deep circuits (not feasible with NISQ technology).

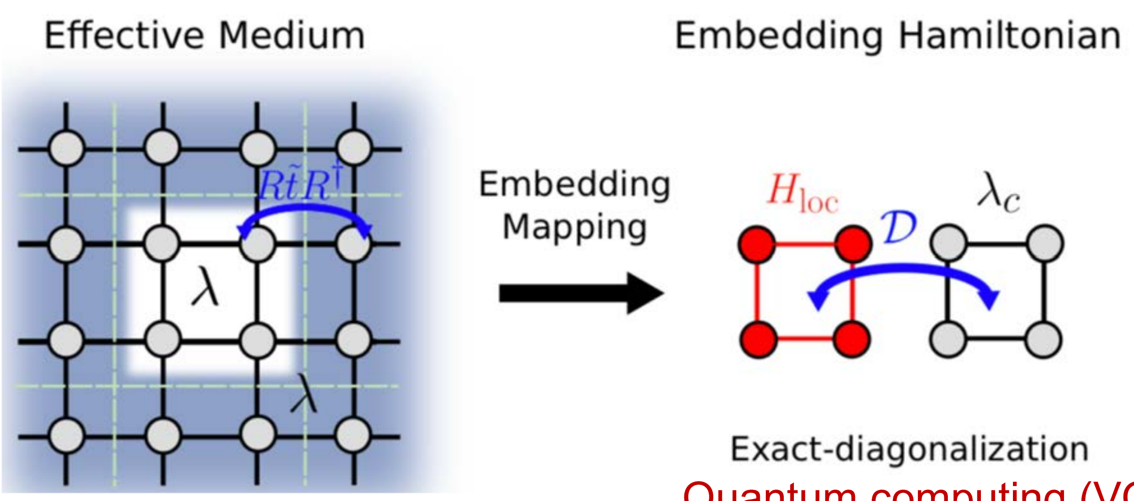
Richard Feynman

Variational optimization on NISQ devices

- Trade deep circuits for many circuit evaluations
- Develop hybrid quantum-classical algorithms
- Optimization problem:
  - minimize energy over variational states $|\psi(\{\theta_n\})\rangle$
  - Prepare target state using QC gates and measure energy
  - Classically optimize parameters (e.g., gradient descent)

$$\Psi_T = \prod_{b=1}^{S}\left[U_U\left(\frac{\theta_U^b}{2}\right)U_h(\theta_h^b)U_v(\theta_v^b)U_U\left(\frac{\theta_U^b}{2}\right)\right]\Psi_I$$

Our approach: solve effective embedding Hamiltonian representing infinite lattice model



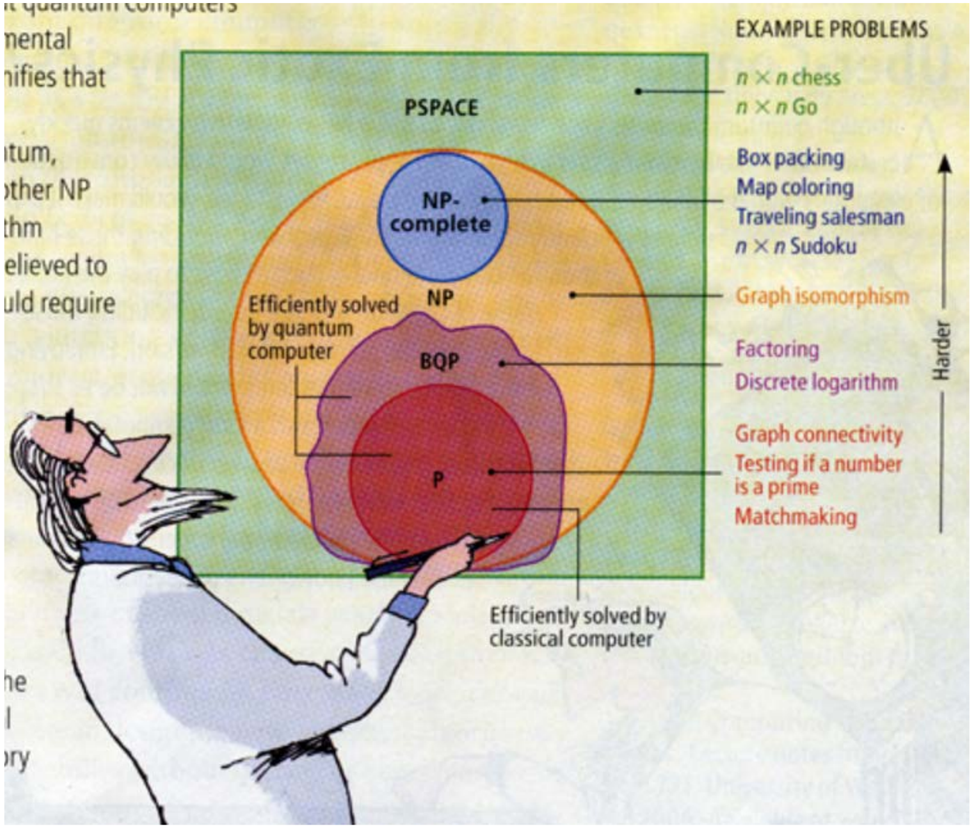
Quantum computing (VQE)

[1] Wecker et al., PRA (2015).
[2] Lee et al. arXiv (2018).

How powerful is a quantum computer

- Complexity classes and how does a QC fit in
  - BQP = Bounded-error Quantum Polynomial time

Matchmaking:
”Given *n* men and *n* women, where each person has ranked all members of the opposite sex in order of preference, marry the men and women together such that there are no two people of opposite sex who would both rather have each other than their current partners.”



Traveling Salesman:
”Given a list of cities and the distances between each pair of cities, what is the shortest possible route that visits each city and returns to the origin city?"

- QC can solve problems outside P, but not outside PSPACE
- Easy NP problems are natural targets

[1] S. Aaronson, Scientific American (2008).

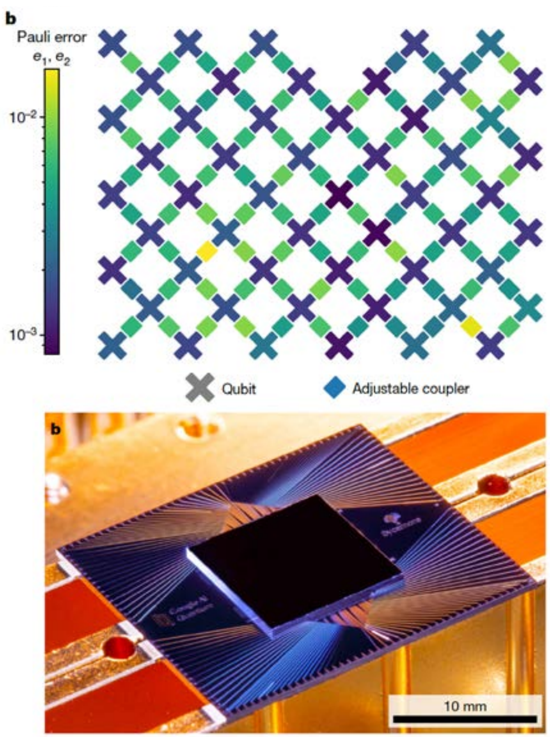
WHAT IS ALL THE HYPE ABOUT?

Google's quantum supremacy experiment

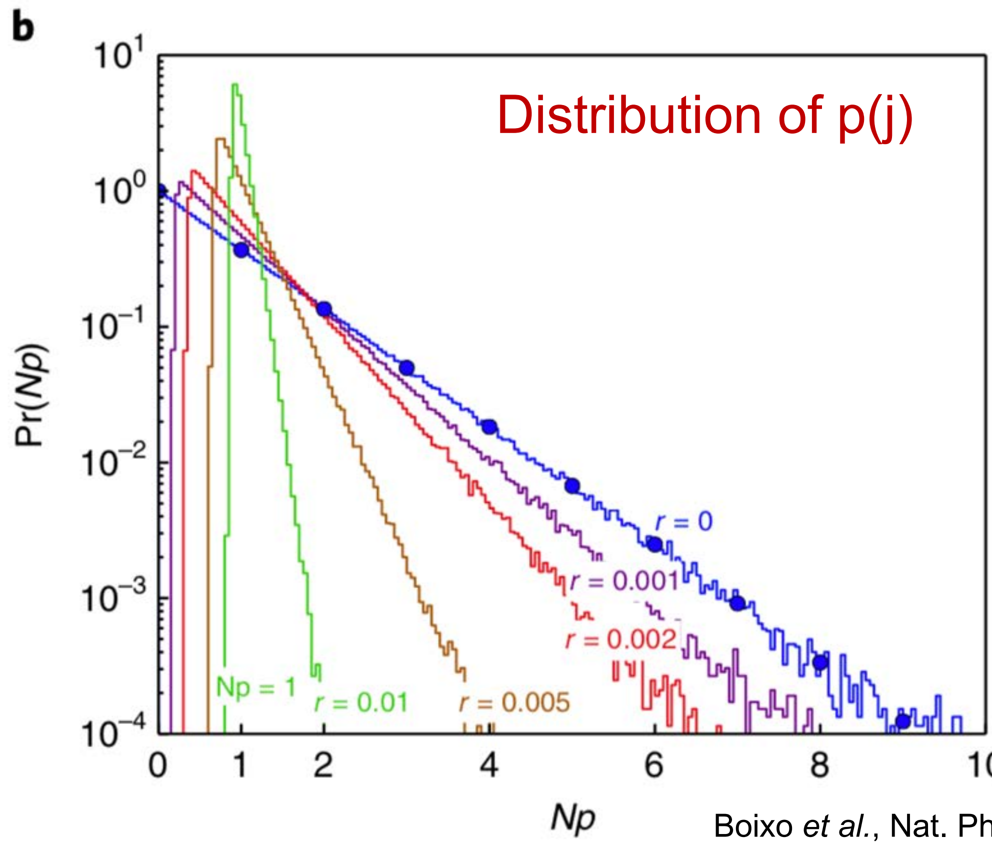
- Task of sampling the output of a pseudo-random quantum circuit

$$U_{\mathrm{rand}}(\alpha)|00\cdots\rangle = \sum_{j=1}^{2^n} a_j |j\rangle \Longrightarrow p(j) = |a_j|^2$$

Probability for bitstring j={|000..>, |100..>, …} to occur (interference!)



Martinis *et al.*, Nature (2019)

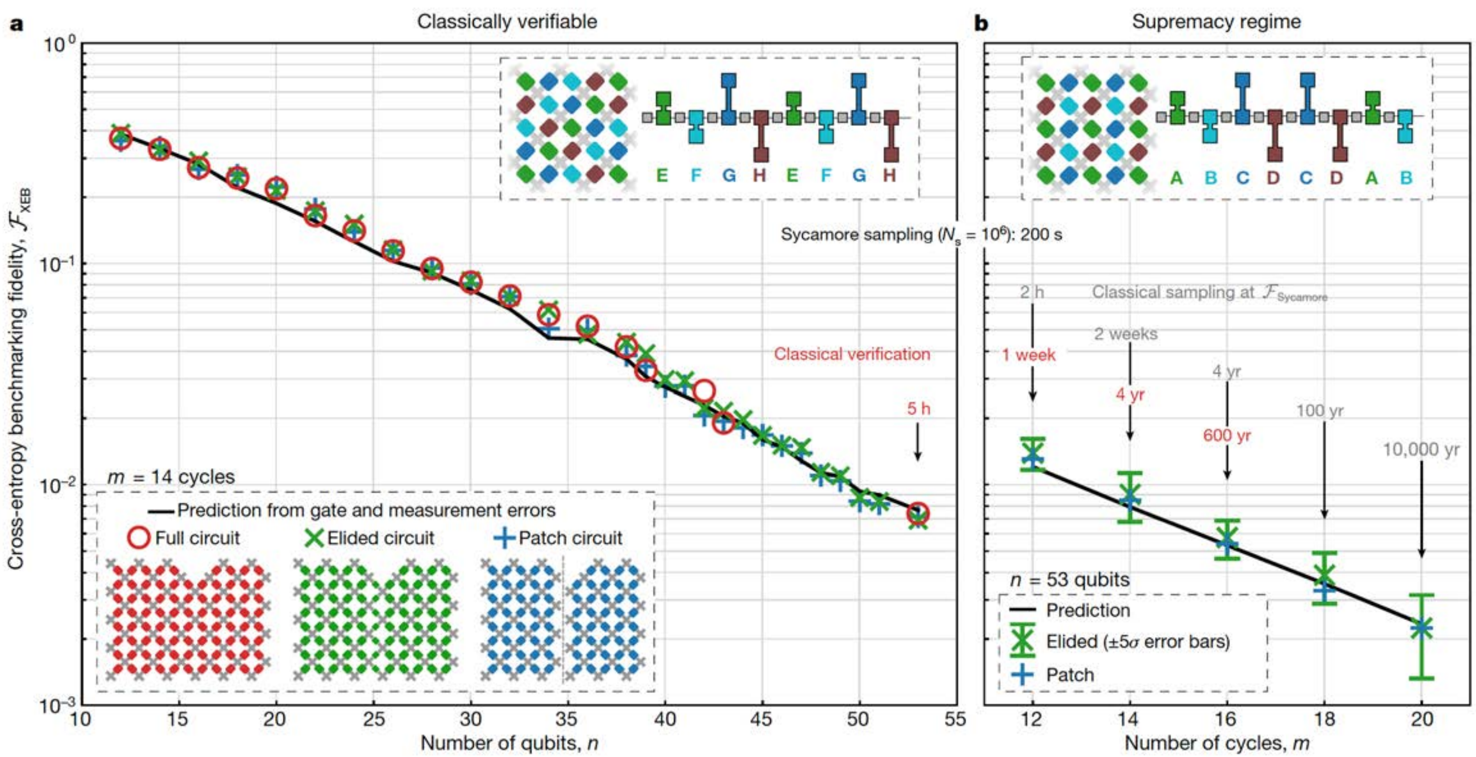


Boixo *et al.*, Nat. Phys. (2018)

Google's quantum supremacy experiment

- Distribution of probabilities $p(j)$: $\mathcal{P}_{PT}(p) = De^{-Dp}$ with $D = 2^n$
- For many qubit errors, uniform distribution emerges $\mathcal{P}_u(p) = \delta(p - D^{-1})$
- Cross-entropy $\mathcal{F}_{\mathrm{XEB}} = 2^n \langle P(x_i) \rangle_i - 1$ is distance measure of $|\mathcal{P}_{QC} - \mathcal{P}_u|$

In 200 sec, the QC produced bitstring probabilities that were not uniform. Classical computer needs much longer. Quantum supremacy!



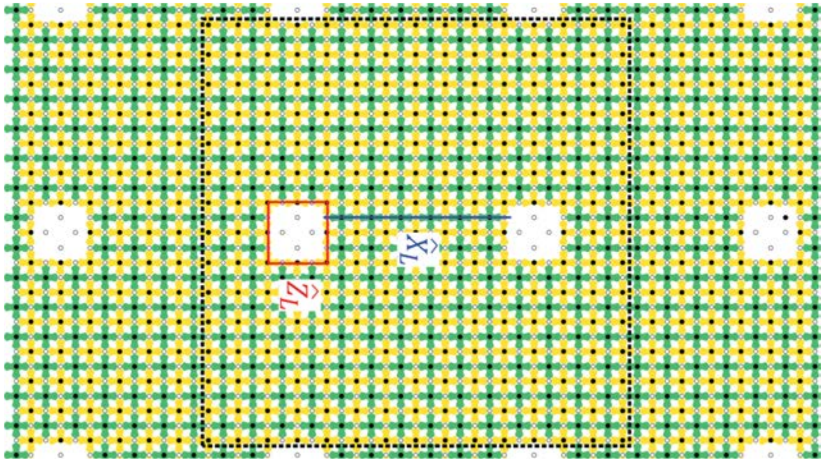
Martinis *et al.*, Nature (2019)

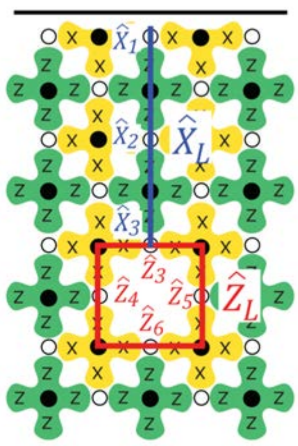
What's next after quantum supremacy?

The path to full fledged quantum computer, capable of performing error correction is long. Many near-term goals along the way.

- Near-term: noisy intermediate scale quantum computing NISQ era
  - Devices with more qubits (100-1000) and better quality (<0.1% error)
  - Circuit depth limited by: max gate number x error rate = 1
- Long term: implement error-correction schemes
  - Main idea: encode 1 logical qubit in $N \gg 1$ physical qubits
  - Fully fault-tolerant QC necessary for many algorithms
  - Topological qubits? Would be more protected against noise

Figure from [1].

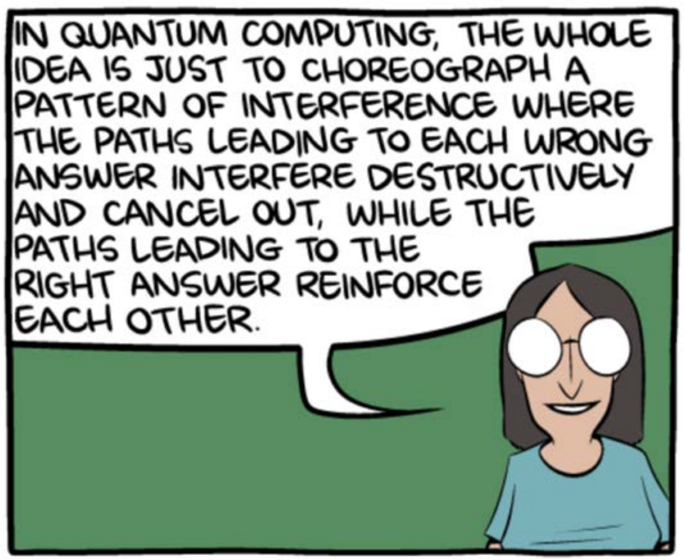




Stabilizer circuits:
[1] Fowler, Martinis, Cleland et al., PRA (2012).
[2] Kitaev (1997).
[2] Bravyi, Kitaev (1998).
[3] Gottesmann, Preskill (1997).
[3] Raussendorf, Harrington (2006).

Summary

- New NISQ era of quantum computing has just begun
- Quantum supremacy achieved
- Many near-term applications envisioned → quantum gold rush
- Long term goal: full fledged QC with error correction
- Many interesting and challenging open questions in the field!



Thanks for your attention!