Quantum Computation: Entangling with the Future

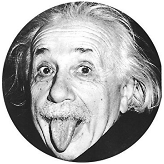
Zhang Jiang

QuAIL, NASA Ames Research Center, Moffett Field, CA
SGT Inc., Greenbelt, MD

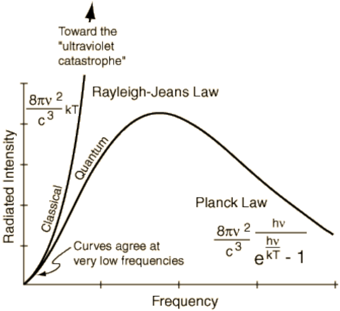
Visa Research, Palo Alto

I: Quantum Mechanics

The Origin of Quantum Mechanics



Quantum mechanics gradually arose from Max Planck's solution in 1900 to the black-body radiation problem and Albert Einstein's 1905 paper which offered a quantum-based theory to explain the photoelectric effect.

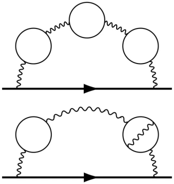


$$E = h\nu$$

The Most Accurate Physical Theory

Quantum Electrodynamics:

The agreement of the fine-structure constant is found within ten parts in a billion (10^{-8}), based on the comparison of the electron anomalous magnetic dipole moment and atom recoil measurements.

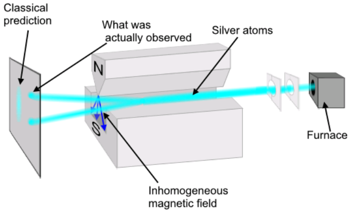


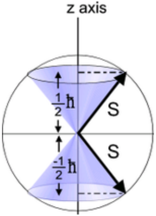
Atomic Quantum Clock:

In March 2008, physicists at NIST described a quantum logic clock based on individual ions of beryllium and aluminium. It was the world's most precise clock which neither gaining nor losing time at a rate that would exceed a second in over a billion years.

Stern-Gerlach Experiment

In 1921, Stern and Gerlach performed an experiment, where silver atoms travel through an inhomogeneous magnetic field and are deflected up or down depending on their spin.





Quantization of Electron Spin:

Electrons are spin-$1/2$ particles; they have only two possible spin angular momentum values measured along any axis, $+\hbar/2$ or $-\hbar/2$, a purely quantum mechanical phenomenon.

Schrödinger's Cat and Quantum Superposition

Schrödinger's cat is either alive or dead until measurements are made.

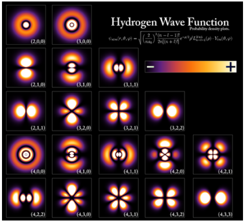
A quantum state is a superposition of many basis states

$$|\psi\rangle = a_0 |\psi_0\rangle + a_1 |\psi_1\rangle + a_2 |\psi_2\rangle + \cdots ,$$

where the amplitudes $a_0, a_1, a_2, \ldots$ are complex numbers satisfying $\sum_j |a_j|^2 = 1$. It evolves under Schrödinger's equation

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

The quantum state "collapse" to a basis state $|j\rangle$ with probability $|a_j|^2$ when a measurement in that basis is made.

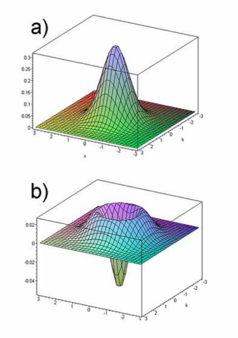


Hydrogen Atom:

Solution to Schrödinger's equation at different energy levels. The brighter areas represent a higher probability of finding an electron. The energy are quantized and take only *discrete* values.

Quantum mechanics is intrinsically *probabilistic*, however, quantum correlations *cannot* be interpreted by classical probability theory.

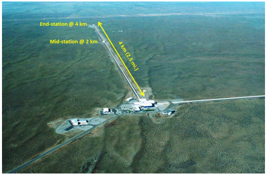
Quantum quasiprobability distribution can take *negative* values: a) zero-photon state (classical); b) one-photon state (quantum).

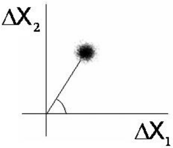


The only thing that is certain in quantum mechanics is the uncertainty principle by Heisenberg

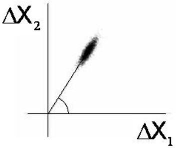
$$\Delta p \, \Delta x \geq \frac{\hbar}{2} \, .$$

Applications dependent on the uncertainty principle include extremely low-noise technology such as that required in gravitational wave interferometers.





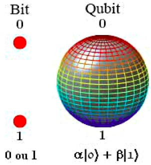
Coherent Light



Squeezed Coherent Light

Bit and Qubit:

The basic element of a quantum computer is a two-dimensional quantum system called qubit, namely quantum bit.



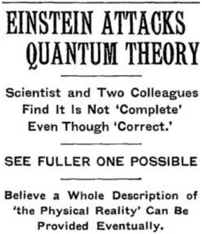
Quantum State-Space Is Large:

There are 2^n basis state for n qubits

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \ , \quad \text{where } \{x_1, x_2, \ldots, x_n\} = \{0,1\}^n \ .$$

One need 2^n complex numbers to specify a quantum state, which exceeds the total number of atoms in the universe for $n \simeq 300$ qubits.

Quantum Entanglement


EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Einstein famously derided entanglement as "spooky action at a distance."

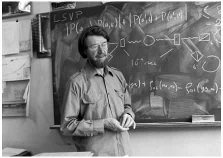
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(\, |00\rangle + |11\rangle \,\right)$$

Bell-CHSH Inequality:

$$C(a,b) + C(a,b') + C(a',b) - C(a',b') \leq 2$$

where

$$C(a,b) = \int A(a,\lambda)B(b,\lambda)p(\lambda)d\lambda.$$



Quantum mechanics can violate these constraints, and thus NO physical theory of local hidden variables can ever reproduce quantum mechanics.

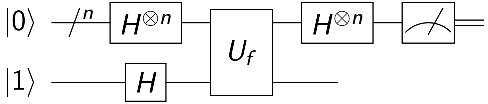
II: Quantum Algorithms

Deutsch-Jozsa Algorithm and Quantum Parallelism

We are given a black box known as an *oracle* that implements

$$f : \{0,1\}^n \rightarrow \{0,1\}.$$

The function f is either constant or balanced (returns 0 for half of the input domain); the task then is to determine if f is constant or balanced.



$$|00\cdots 0\rangle \xRightarrow{H^{\otimes n}} \sum_{x=0}^{2^n-1} |x\rangle$$

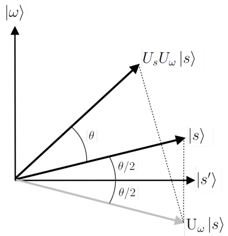
$$U_f|x\rangle \otimes (|0\rangle - |1\rangle) = |x\rangle \otimes (|f(x)\rangle - |1 \oplus f(x)\rangle) = (-1)^{f(x)}|x\rangle \otimes (|0\rangle - |1\rangle)$$

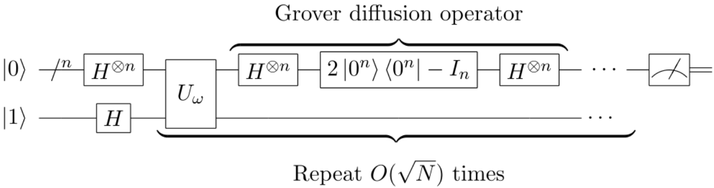
Finally, we examine the probability of measuring $|00\cdots 0\rangle$, which evaluates to 1 if f is constant (constructive interference) and 0 if f is balanced (destructive interference).

Grover's algorithm searches for a needle ω in a haystack, achieving a quadratic quantum speedup (optimal) over the best classical algorithms.

The oracle U_ω flips the sign of the marked item, and the Grover diffusion operator is:

$$U_s = 2\,|s\rangle\langle s| - I\,,\quad \text{where } |s\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle.$$

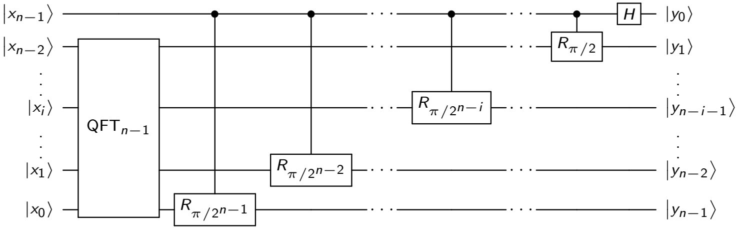




Quantum Fourier Transformation

The quantum Fourier transform is a part of many quantum algorithms.

$$|y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{\frac{2\pi ixy}{N}} |x\rangle$$



It can be implemented efficiently as a quantum circuit consisting of only $\mathcal{O}\left((\log N)^2\right)$ basic quantum gates, exponentially faster than classical discrete Fourier transformation.

Shor's Algorithm for Integer Factorization

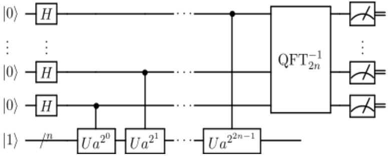
Shor's algorithm could be used to break public-key cryptography schemes such as the widely used RSA scheme. It takes quantum gates of order

$$O\big((\log N)^2(\log\log N)(\log\log\log N)\big)\,.$$

In contrast, the general number field sieve (best classical algorithm) works in sub-exponential time

$$O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)\,.$$

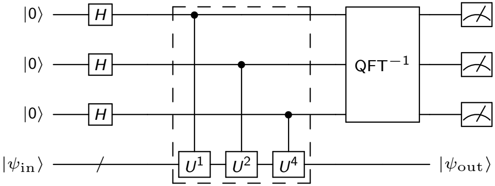
1. Turn the factoring problem into finding the period of a function
2. Find the period using the quantum Fourier transform (responsible for the quantum speedup)



Quantum Phase Estimation Algorithm

Quantum phase estimation makes it possible to estimate the phase that a unitary transformation adds to one of its eigenvectors.

$$U\,|\psi_j\rangle = e^{iu_j}\,|\psi_j\rangle$$
$$U^k\,|\psi_j\rangle = e^{iku_j}\,|\psi_j\rangle$$
$$|\psi_{\mathrm{reg}}\rangle = \frac{1}{\sqrt{R}}\sum_{r=0}^{R-1}|r\rangle$$



$$\boxed{\left(|\psi_j\rangle\otimes|\psi_{\mathrm{reg}}\rangle\right)\Longrightarrow\frac{1}{\sqrt{R}}\;|\psi_j\rangle\otimes\left(\sum_r e^{iru_j}\,|r\rangle\right)}$$

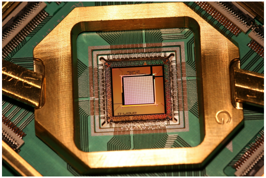
It is used as a subroutine in several applications such as order finding, factoring and discrete logarithm, and quantum chemistry.

Adiabatic Quantum Computation

A physical system remains in its instantaneous eigenstate if a given perturbation is acting on it slowly enough.

$$\hat{H}(s) = (1-s)\hat{H}_0 + s\hat{H}_{\mathrm{final}}, \quad 0 \leq s \leq 1$$

The minimum gap of $\hat{H}(s)$ determines computational time; adiabatic quantum computation is equivalent to standard quantum computation.

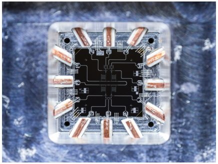


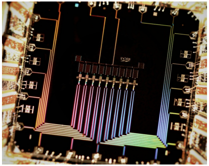
A chip constructed by D-Wave Systems Inc. to operate as a 1000-qubit superconducting adiabatic quantum optimization processor.

III: Implementation

DiVincenzo Criteria for Scalable Quantum Computation

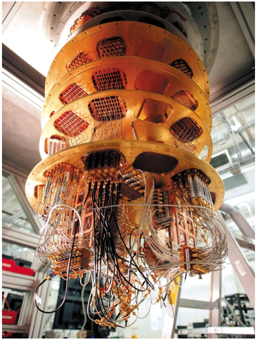
1. Identification of well-defined qubits
2. Reliable state preparation
3. Low decoherence
4. Accurate quantum gate operations
5. Strong quantum measurements





g-mon and x-mon qubits from Google's quantum artificial intelligence laboratory

A $^3\mathrm{He}/^4\mathrm{He}$ dilution refrigerator cryogenic device

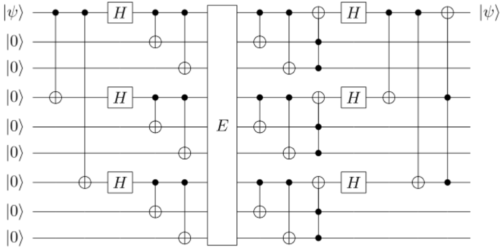


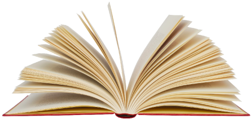
Quantum Error Correction

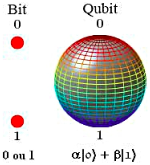
Two Potential Obstacles:

1. It is impossible to clone an unknown quantum state.
2. Quantum states are continuous; there are infinitely many of errors.

An example of quantum error-correcting code that corrects both the sign flip and bit flip errors.

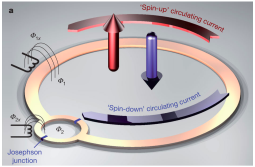


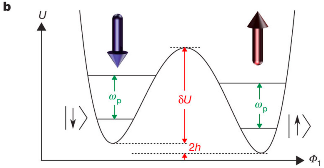




Superconducting Qubits

Industry research in superconducting quantum computing is conducted by Google, IBM, Intel, and D-Wave Systems, partly due to its scalability.





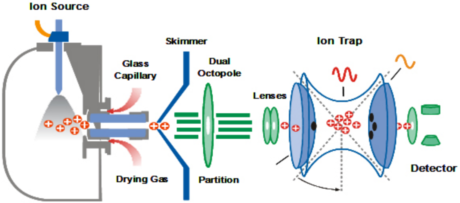
In a superconductor, the basic charge carriers are pairs of electrons (known as Cooper pairs). The devices are cooled down in dilution refrigerators below 100mK.

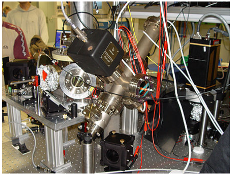
A junction is a weak connection between two pieces of a superconducting wire, usually implemented as a thin layer of insulator.

M. W. Johnson et al., "Quantum annealing with manufactured spins", Nature **473**, 194–198 (2011)

Trapped Ions

An ion trap is a combination of electric or magnetic fields used to capture charged particles, often in a system isolated from an external environment.



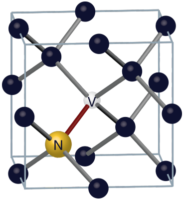


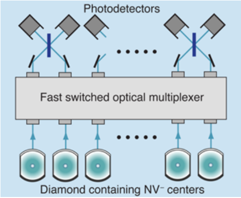
Ions, or charged atomic particles, can be confined and suspended using electromagnetic fields. Lasers are applied to induce single qubit operations or for entanglement between qubits. Initialization and measurement precision $> 99.9\%$, gate fidelity $> 99\%$

Nitrogen-Vacancy Centers in Diamond

How about a quantum computer in room temperature?

The nitrogen-vacancy center is a point defect in the diamond lattice. It consists of a nearest-neighbor pair of a nitrogen atom.



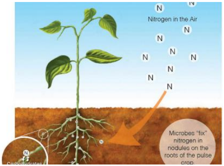


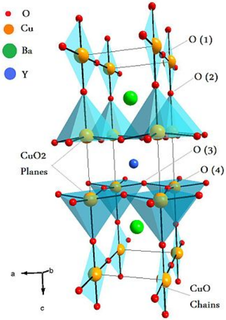
Larger arrays of diamond center qubits could be linked via a fast-switched optical multiplexer, in readiness for the final measurement step.

IV: Commercialization

Simulating Quantum Systems

Nitrogen Fixation: Haber-Bosch process, used to manufacture ammonia for fertilizer production, consumes two percent of the world's energy. Devising a more efficient catalyst could be extremely valuable.





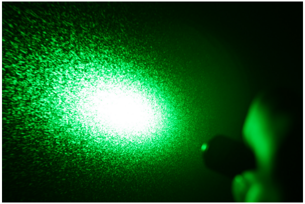
High-T_c Superconductor & Chemistry:

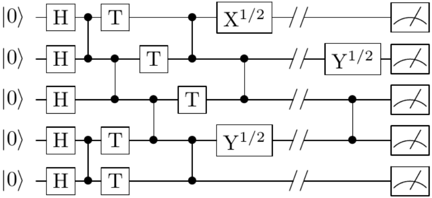
A widely accepted theory for high-T_c superconductor still lacks after 30 years of intense research.

A quantum computer can give more accurate estimates of the energy differences in chemical reactions and thus give better estimates of the reaction rates.

Quantum Sampling

Sampling from probability distributions is widely used in statistics and machine learning. Using a circuit of just 7×7 qubits in 25 layers of high-fidelity quantum gates, it will be possible to sample from probability distributions that are inaccessible classically.



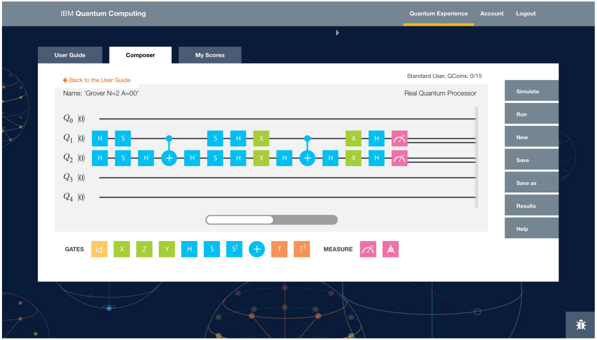


S. Boixo et al., "Characterizing Quantum Supremacy in Near-Term Devices", arXiv:1608.00263 (2016)

Cloud Quantum Computing

IBM Quantum Experience allows building and running quantum algorithms on a 5 superconducting qubits processor.

Google also plan to support such endeavor by offering access to Google's quantum processors via cloud services.



Conclusion

"If early quantum-computing devices can offer even a modest increase in computing speed or power, early adopters will reap the rewards. Rival companies would face high entry barriers to match the same quality of services and products, because few experts can write quantum algorithms, and businesses need time to tailor new algorithms."

Thanks for your attention!

M. Mohseni et al., "Commercialize quantum technologies in five years", Nature News **543**, 171 (2017)