Quantum Computing
(from the unthinkable to the inevitable)

Quantum Computing May Lead to Revolutionary Breakthroughs

C Patvardhan
Professor, Electrical Engineering, Dayalbagh Educational Institute
Quantum computing

• A quantum computer is a machine designed to use the principles of quantum mechanics to do things which are fundamentally impossible for any computer which only uses classical physics.
• **Brian Krzanich**, Chief Executive of Intel, said in a blog article in September 2015: “I’m excited about the role that Intel’s greatest minds and expertise can play in shaping this impactful technology, and I hope you are too. **Quantum computing holds the promise of solving complex problems that are practically insurmountable today, changing the world for the better.** That’s a technology I think we’ll all be incredibly proud to play a part in developing.”

• **Vern Brownell**, Chief Executive of D-Wave, believes the quantum computing era has begun. In an interview with CIO.com (June 2016), Brownell said: **“We’re at the dawn of this quantum computing age. We believe we’re right on the cusp of providing capabilities you can’t get with classical computing... We’re at the bleeding edge today. It’s a very exciting time to be in the middle of all this.”**
The father of quantum computing sees it as a fundamentally new way of harnessing nature

“I OCCASIONALLY go down and look at the experiments being done in the basement of the Clarendon Lab, and it’s incredible.” David Deutsch, of the University of Oxford, is the sort of theoretical physicist who comes up with ideas that shock and confound his experimentalist colleagues—and then seems rather endearingly shocked and confounded by what they are doing. “Last year I saw their ion-trap experiment, where they were experimenting on a single calcium atom,” he says. “The idea of not just accessing but manipulating it, in incredibly subtle ways, is something I totally assumed would never happen. Now they do it routinely.”

Such trapped ions are candidates for the innards of eventual powerful quantum computers. These will be the crowning glory of the quantum theory of computation, a field founded on a 1985 paper by Dr Deutsch. He thinks the widely predicted “quantum supremacy” that eventually puts a quantum computation incontrovertibly ahead of a classical one will be momentous for scientists and laymen alike. He brushes off the fervent debate about whether the commercially available D-Wave computer offers a speed advantage. “If it works, it works in a completely different way that cannot be expressed classically. This is a fundamentally new way of harnessing nature. To me, it’s secondary how fast it is.”
Key ingredients of quantum mechanics

- Quantum mechanics has certain bizarre features which do not occur in standard, or “classical” physics, such as:
  - **Superposition.** If a system can be in state A or state B, it can also be in a “mixture” of the two states. If we measure it, we see either A or B, probabilistically.
  - **Collapse.** Any further measurements will give the same result.
  - **Entanglement.** There exist systems of multiple parts which cannot be described only in terms of their constituent parts.
  - **Uncertainty.** There are pairs of measurements where greater certainty of the outcome of one measurement implies greater uncertainty of the outcome of the other measurement.
- The basic idea behind quantum computing is to use these effects to our advantage.
“I think I can safely say that nobody understands quantum mechanics” - Feynman

1982 - Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics.

1985 - David Deutsch developed the quantum Turing machine, showing that quantum circuits are universal.

1994 - Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.

1997 - Lov Grover develops a quantum search algorithm with $O(\sqrt{N})$ complexity
Classical mechanics is the mechanics of everyday objects like tables and chairs

1. An object in motion tends to stay in motion.
2. Force equals mass times acceleration
3. For every action there is an equal and opposite reaction.

Sir Isaac Newton
Classical mechanics reigned as the dominant theory of mechanics for centuries

1687 – Newton’s *Philosophiae Mathematica*

1788 – Lagrange’s *Mecanique Analytique*

1834 – Hamiltonian mechanics

1864 – Maxwell’s equations

1900 – Boltzmann’s entropy equation
The two-slit experiment is one of the classic validations of the predictions of quantum theory.

The Two Slit Experiment
- the one slit experiment
- the two slit experiment
- the results
- the classical “explanation”
- the test
- the quantum explanation
- curioser and curioser

Experiments on interference made with particle rays have given brilliant proof that the wave character of the phenomena of motion as assumed by the theory does, really, correspond to the facts. -A. Einstein
In the one-slit experiment, particles that pass through the single slit produce an image on the detector.

What happens if we use two slits instead of only one?
If we use two slits, we might expect to obtain the sum of two single-slit distributions...

Warning: the “expected result” presented by this slide is patently false
...but in reality, we obtain an interference pattern.

The Two Slit Experiment

Particle emitter → Particles → Detector

Actual result: interference pattern.

Question: Is this a quantum phenomenon?
A clever physicist might attempt to explain this result as the consequence of “crowd waves”...

The Classical “Explanation” - Interference phenomena are caused by disturbances propagating through huge numbers of water particles

Warning: the “classical ‘explanation’” presented on this slide is patently false
...but an even cleverer physicist can test this hypothesis by configuring the emitter to emit the particles one at a time.

The Two Slit Experiment

Result: Interference pattern remains!
The quantum mechanical explanation is that each particle passes through both slits and interferes *with itself*. The wave function of each particle is a probability wave which produces a probability interference pattern when it passes through the two slits.

The wave function of each particle is a probability wave which produces a probability interference pattern when it passes through the two slits.
If a measurement device is placed on one of the slits, then the interference pattern disappears.
The measurement device has collapsed the wave function, leading to a loss of interference.
Quantum mechanics makes several revolutionary claims about the fundamental behavior of particles.

The claims of quantum mechanics:

1. Particles act like waves.
   Particles can interfere with *themselves*.
2. Particles do whatever they want.
   There is a non-zero probability of finding a particle essentially *anywhere* in the universe.
3. Measurement is *inherently* probabilistic.
   No supplemental knowledge will make measurement deterministic.

"Anyone who is not shocked by quantum mechanics has not understood it." - Niels Bohr
Quantum mechanics was developed to explain some new results and developed into the most successful physical theory in history.
Although quantum mechanics applies to all objects, the effects of quantum mechanics are most noticeable only for very small objects.

How small is very small?

1 meter    Looks classical
1 millimeter    Looks classical
1 micrometer    Looks classical
1 nanometer    Looks quantum!
Nonetheless, quantum mechanics is still very important.

How important is very important?

Without quantum mechanics:

- Many biological reactions would not occur.
- Chemical bonding would be impossible.
- All atoms would be unstable.
- Life does not exist
- All molecules disintegrate
- Universe explodes
- Minimal consequences

Neil Shenvi’s dissertation title: *Vanity of Vanities, All is Vanity*
The laws of quantum mechanics are founded upon several fundamental postulates

The Fundamental Postulates of Quantum Mechanics:

Postulate 1: All information about a system is provided by the system’s wave function.

Postulate 2: The motion of a nonrelativistic particle is governed by the Schrodinger equation

Postulate 3: Measurement of a system is associated with a linear, Hermitian operator
**Postulate 1:** All information about a system is provided by the system’s wave function.

Interesting facts about the **wavefunction**:
1. The **wavefunction** can be positive, negative, or complex-valued.
2. The **squared amplitude** of the wavefunction at position $x$ is equal to the **probability** of observing the particle at position $x$.
3. The wave function can change with time.
4. The existence of a wavefunction implies particle-wave duality.
The Weirdness of Postulate 1: Quantum particles are usually delocalized, meaning they do not have a well-specified position.
The Weirdness of Postulate 1: At a given instant in time, the position and momentum of a particle cannot both be known with absolute certainty.

This consequence is known as Heisenberg’s uncertainty principle.
The Weirdness of Postulate 1: a particle can be put into a superposition of multiple states at once.

Classical elephant:
Valid states:
- Gray
- Multicolored

Quantum elephant:
Valid states:
- Gray
- Multicolored

Gray AND Multicolored
Postulate 2: The motion of a nonrelativistic particle is governed by the Schrödinger equation

Time-dependent S.E.: 
\[ i\hbar \frac{\partial}{\partial t} \left| \Psi(t) \right\rangle = \hat{H} \left| \Psi(t) \right\rangle \]

Time-dependent S.E.: 
\[ \hat{H} \left| \Psi \right\rangle = E \left| \Psi \right\rangle \]

Molecular S.E.: 
\[ \left( -\frac{\hbar^2}{2m} \frac{d^2}{dx^2} + \hat{V}(x) \right) \Psi(x) = E \Psi(x) \]

Interesting facts about the Schrödinger Equation:
1. It is a wave equation whose solutions display interference effects.
2. It implies that time evolution is unitary and therefore reversible.
3. It is very, very difficult to solve for large systems (i.e. more than three particles).
The Weirdness of Postulate 2: A quantum mechanical particle can tunnel through barriers rather than going over them.

Classical ball does not have enough energy to climb hill.

Quantum ball tunnels through hill despite insufficient energy.

This effect is the basis for the scanning tunneling electron microscope (STEM)
The Weirdness of Postulate 2: Quantum particles take \textit{all} paths.

Classical mouse

Classical particles take a single path specified by Newton’s equations.

Quantum mouse

The Schrodinger equation indicates that there is a nonzero probability for a particle to take any path.

This consequence is stated rigorously in Feynmann’s path integral formulation of quantum mechanics.
Postulate 3: Measurement of a quantum mechanical system is associated with some linear, Hermitian operator $\hat{O}$.

\[
\langle \hat{O} \rangle = \langle \Psi | \hat{O} | \Psi \rangle \\
\langle \hat{O} \rangle = \int dx \, \Psi^* (x) \hat{O}(x) \Psi (x)
\]

Interesting facts about the measurement postulate:
1. It implies that certain properties can only achieve a discrete set of measured values
2. It implies that measurement is inherently probabilistic.
3. It implies that measurement necessarily alters the observed system.
The Weirdness of Postulate 3: Even if the exact wave function is known, the outcome of measurement is inherently probabilistic.

**Classical Elephant:**

**Before measurement**

**After measurement**

For a known state, outcome is deterministic.

---

**Quantum Elephant:**

**Before measurement**

**After measurement**

For a known state, outcome is probabilistic.

Or
The Weirdness of Postulate 3: Measurement necessarily alters the observed system

Classical Elephant:

Before measurement

After measurement

State of the system is unchanged by measurement.

Quantum Elephant:

Measurement changes the state of the system.
The Weirdness of Postulate 3: Properties are actions to be performed, not labels to be read

Classical Elephant:

Position = here
Color = grey
Size = large

The ‘position’ of an object exists independently of measurement and is simply ‘read’ by the observer

Quantum Elephant:

‘Position’ is an action performed on an object which produces some particular result

In other words, properties like position or momentum do not exist independent of measurement! (*unless you’re a neorealist…)*
Quantum mechanics is:
1. Incomplete
2. Incorrect
3. Or both

Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. Quantum theory says a lot, but does not really bring us any closer to the secret of the Old One. I, at any rate, am convinced that He does not throw dice. - A. Einstein

Quantum Mechanics: Real Black Magic Calculus. - A. Einstein
The Bell experiment demonstrates that local realism is false; either locality or realism must be jettisoned.

The Bell experiment demands that we choose one (and only one) of the following principles can be valid:

- **Locality** - the principle that effects cannot propagate faster than the speed of light.

- **Realism** - the principle that objects have properties independent of measurement.

**Warning:** 4 out of 5 physicists recommend keeping locality.
Given the weirdness of quantum mechanics, the obvious question is: why does reality appear so normal?

QM tells me that this is reality:

\[ |\Psi\rangle - |TH\rangle \]

But all I ever see is:
There are three major interpretations of quantum mechanics: Copenhagen, neorealist, and many-worlds.

The Copenhagen interpretation: measurement induces wavefunction collapse.

Neorealist: hidden variables or pilot waves produce nonlocal phenomena.

Many-worlds: measurement leads to bifurcation of multiverse.
Quantum mechanics has many important implications for epistemology and metaphysics

- The possibility of almost anything
- The absence of causality/determinism
- The role of human consciousness
- The limits of human knowledge
- The cognitive dissonance of reality
First, quantum mechanics implies that almost no event is strictly impossible.

Classical physics

Quantum physics

“the random nature of quantum physics means that there is always a minuscule, but nonzero, chance of anything occurring, including that the new collider could spit out man-eating dragons [emph. added]” - physicist Alvaro de Rujula of CERN regarding the Large Hadron Collider, quoted by Dennis Overbye, NYTimes 4/15/08
Second, quantum mechanics abrogates notions of causality and (human?) determinism. Classical physics rigorously provides an answer to the question “what caused this event?”

Physics no longer rigorously provides an answer to the question “what caused this event?”
Third, within the Copenhagen interpretation, human consciousness appears to have a distinct role.

When does the wave function collapse during measurement?

Wavefunction….wavefunction…wavefunction…………particle!

“The very study of the physical world leads to the conclusion that the concept of consciousness is an ultimate reality” “it follows that the being with a consciousness must have a different role in quantum mechanics than the inanimate object” – physicist Eugene Wigner, Nobel laureate and founder of quantum mechanics
Fourth, the fact that the wavefunction is the ultimate reality implies that there is a severe limit to human knowledge.

“…classical mechanics took to superficial a view of the world: it dealt with appearances. However, quantum mechanics accepts that appearances are the manifestation of a deeper structure (the wavefunction, the amplitude of the state, not the state itself)” – Peter Atkins
Finally, quantum mechanics challenges our assumption that ultimate reality will accord with our natural intuition about what is reasonable and normal.

I think it is safe to say that no one understands quantum mechanics. *Do not keep saying to yourself, if you can possibly avoid it, 'But how can it possibly be like that?'* … Nobody knows how it can be like that. – Richard Feynman
What effect does QM have on the fundamental assumptions of science?

1. Rationality of the world
2. Efficacy of human reason
3. Metaphysical realism
4. Regularity of universe
5. Spatial uniformity of universe
6. Temporal uniformity of universe
7. Causality
8. Contingency of universe
9. Desacralization of universe
10. Methodological reductionism (Occam’s razor)
11. Value of scientific enterprise
12. Validity of inductive reasoning
13. Truthfulness of other scientists
It makes things complicated…

1. Rationality of the world
2. Efficacy of human reason
3. Metaphysical realism
4. Regularity of universe
5. Spatial uniformity of universe
6. Temporal uniformity of universe
7. Causality
8. Contingency of universe
9. Desacralization of universe
10. Methodological reductionism (Occam’s razor)
11. Value of scientific enterprise
12. Validity of inductive reasoning
13. Truthfulness of other scientists

Weirdness of Quantum mechanics

Copenhagen interpretation

EPR Experiment: Pick one (only)

Neo-realism

Probabilistic nature of QM
The qubit: the basic building-block of quantum computers

- Quantum mechanics deals with very small systems, like atoms or photons ("particles of light").
- A quantum system which has two distinct states is called a qubit.
- Just as classical computers operate on bits, quantum computers operate on qubits.
- For example, one property of a photon is polarisation: a photon can be either vertically or horizontally polarized (" or !), so this gives us a qubit.
Even if we move one of the qubits to the Moon, the global state of the two qubits cannot be described solely in terms of the individual state of each of them!

In particular, if we measure one of the qubits, this apparently instantaneously affects the other one.
• Born a century ago, this theory is the rule book for what happens at atomic scales
  • Provides explanations for everything from the layout of the periodic table to the zoo of particles spraying out of atom-smashers.
  • Has guided the development of everyday technologies from lasers to MRI machines.
  • Put a solid foundation under astrophysicists’ musings about unknowables such as the interiors of black holes and the dawn of the universe.

• Revealed by a few surprising discoveries, such as that atoms absorb and emit energy only in packets of discrete sizes (quanta), and that light and matter can act as both waves and particles, it is modern physics’ greatest triumph.

• Particles be in two states at once, as with the atoms in an atomic clock; sometimes two of them, separated by a great distance, seemingly sense something about each other’s condition, a situation called entanglement.

• A particle’s exact position or state is never certain until a measurement is made; there are only higher or lower likelihoods of a given outcome, and the measurement changes the situation irrevocably.
Utilizing Quantum Mechanics – II revolution

• The most counterintuitive quantum-mechanical predictions are being harnessed
  • to make measurements of staggering precision,
  • to generate uncrackable codes and to form the basis of impenetrable communications networks.

• Quantum computers may eventually crunch through currently unapproachable problems, improving the transmission of electric power or the manufacture of energy-intensive fertilizer, or simply sifting through impractically large data sets.

• However, long before then computing systems that still fall far short of a general-purpose machine are likely to start providing solutions in industries such as finance, energy and aerospace, and even help with things as mundane as recommendation engines.
The dawn of quantum computing

• 1982
  • Nobel Laureate Richard Feynman asked whether quantum physics could be simulated efficiently using a quantum computer.
  • “If you want to make a simulation of nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem, because it doesn’t look so easy.”

• 1985
  • David Deutsch proposes the mathematical concept of the quantum Turing machine to model quantum computation. This put the concept of quantum computing on a sound theoretical footing for the first time.
  • “Computing devices resembling the universal quantum computer can, in principle, be built and would have many remarkable properties not reproducible by any Turing machine.”

• But could a quantum computer actually outperform a classical computer?

• 1992
  • David Deutsch and Richard Jozsa give the first such example.
  • “The quantum computation solves the problem with certainty in exponentially less time than any classical deterministic computation.”
1993

- Ethan Bernstein and Umesh Vazirani show that quantum computers can be significantly faster than classical computers, even if the classical computer is allowed a small probability of error.

1994

- Dan Simon shows that quantum computers can be exponentially faster.
- Peter Shor shows that quantum computers can factorize large integers efficiently. Given an integer \( N = p \times q \) for prime numbers \( p \) and \( q \), Shor’s algorithm outputs \( p \) and \( q \). No efficient classical algorithm for this task is known.

1996

- Lov Grover gives a quantum algorithm which solves unstructured search problem using about \( \sqrt{n} \) queries. The square-root speedup of Grover’s algorithm finds many applications to search and optimization problems.
The dawn of quantum computing (3)

• 1996
  • Seth Lloyd proposes a quantum algorithm which can simulate quantum-mechanical systems.
  • “A quantum computer with a few tens of quantum bits could perform in a few tens of steps simulations that would require Avogadro’s number $[6 \times 10^{23}]$ of memory sites and operations on a classical computer.”
  • Simulating quantum mechanics has applications to drug design, materials science, high-energy physics, . . .
“Typical atoms useful for quantum computation usually need to be at a temperature close to absolute zero (around 1 billionth of a kelvin)”

In 2012 Serge Haroche, a Frenchman, and David J. Wineland, an American, were awarded the Nobel Prize in Physics in Quantum Computing “for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems”.
Goals of Quantum Computing Research

• One goal is to probe the foundations of the theory of computation.
  • What limits are imposed on computation by the fundamental laws of physics, and how can computational power be enhanced by exploiting the structure of these laws?

• Another goal is to extend the theory of communication.
  • What are the ultimate physical limits on the performance of a communication channel, and how might quantum phenomena be harnessed by new communication protocols?

• Yet another challenge is to understand and overcome the quantum effects that constrain how accurately we can monitor and manipulate physical systems.
  • What new strategies can be devised to push back the frontier of quantum-limited measurements, or to control the behavior of intricate quantum systems? Quantum effects seem to compromise our efforts to store, transmit, and process information, because quantum states are highly unstable and cannot be observed without being disturbed.
  • Indeed, as the components of integrated circuits continue to shrink toward the atomic scale, quantum phenomena will pose increasingly serious limitations on the performance of information processing hardware, and one important task of quantum information science will be to illuminate whether and how such obstacles can be overcome.
Good News!

• The fragility of quantum information becomes a very positive feature when it is recognized that eavesdropping on a quantum communication channel necessarily leaves a detectable imprint, so that communicating with qubits provides better privacy than communicating with classical bits.

• Far more astonishing, the intrinsic complexity of quantum information ensures that quantum systems of modest size are endowed with truly vast computational power, so that a quantum computer acting on just hundreds of qubits is capable in principle of performing tasks that could never be performed by conventional digital computers.
Broad Areas of Quantum Information Processing

• **Quantum secure communications**: which offer the prospect of fundamentally secure communication channels (as one could prove through the laws of quantum physics that no information was intercepted). This includes patents relating explicitly to encryption, e.g. quantum key distribution (QKD), as well as transmission systems and components that are specific to quantum communications;

• **Quantum metrology and sensors**: where quantum effects such as entanglement or superposition are exploited in the undertaking of high-resolution and highly sensitive measurements of physical parameters;

• **Quantum simulators**: which enable the accurate modelling of real molecules and materials;

• **Quantum computation**: information processing by using quantum superposition, coherence, decoherence, entanglement, nonlocality and/or teleportation.
But can we actually build one?

• Building a large-scale quantum computer is extremely challenging because of decoherence. If a quantum computer interacts with the outside world and is subject to noise, it can lose its “quantumness” and behave like a classical computer.

• 1995-6:
  • Peter Shor and Andrew Steane devise quantum error-correcting codes which can be used to fight decoherence. The most optimistic current estimates are that a fault-tolerant quantum computer could be built from components which have an error rate of up to about 1%.
QC TODAY

• Quantum computing is no longer in the realm of science fiction, and as the global race to build a quantum computer heats up, the commercial landscape will continue to change, presenting new investment opportunities as a result.

• The promise of quantum computing is both exciting and inspiring.
Di Vincenzo’s Criteria for Quantum Computation and Communication

1. A scalable physical system with well-characterized qubits.
2. The ability to initialize the state of the qubits to a simple fiducial state.
3. Long (relative) decoherence times, much longer than the gate-operation time.
5. A qubit-specific measurement capability.
6. The ability to interconvert stationary and flying qubits.
7. The ability to faithfully transmit flying qubits between specified locations.
Problems to be solved for realization of Quantum Computers

- Identification of the best suitable physical system which allows for scalability, coherence and fast implementation of Quantum Information Processing.
- Engineering and control of quantum mechanical systems far beyond anything achieved so far, in particular concerning reliability, fault tolerance and using error correction.
- Development of a computer architecture taking into account quantum mechanical features.
- Development of interfacing and networking techniques for quantum computers.
- Investigation and development of quantum algorithms and protocols.
- Transfer of academic knowledge about the control and measurement of quantum systems to industry and thus, acquisition of industrial support and interest for developing and providing quantum systems.
Some experimental progress

- 1997-8 Quantum teleportation demonstrated [Innsbruck, Rome, Caltech, ...]
- 1998 Quantum error-correction demonstrated [MIT]
- 2001 Shor’s algorithm factorises 15 = 3^2 × 5 using NMR [IBM]
- 2005 8 qubits controlled in ion trap [Innsbruck]
- 2008 Photonic waveguide quantum circuits demonstrated [Bristol]
- 2010 Entangled states of 14 qubits created in ion trap [Innsbruck]
- 2012 21 = 3 × 7 factorised using quantum optics [Bristol]
- 2012 100s coherence for superconducting electronic qubits [IBM]
- 2013 First publicly-accessible “quantum cloud” [Bristol]
- 2014 Superconducting qubits at fault-tolerant threshold [UCSB]
- 2016 Teleportation in Space MICIUS satellite by China
- 2017 2048 Qubit DWAVE Computer
- 2018 72 Qubit IBM Quantum Computer
Two categories of Quantum Computers

• The first is a **Universal Quantum Computer**. Much like a conventional computing processor, it can perform any kind of quantum computational operation.

• The second is the **Annealing Machine**, which is targeted in solving specific types of optimization problems.

• Constructing a quantum computer with the level of precision required to create, manipulate and measure qubits is extremely challenging.

• Qubits are very sensitive to their local environment and any interactions can result in decoherence, or loss of information.

• There are currently three popular engineering approaches: **Ion-based Qubits**, **Superconducting Qubits** and **Solid-State Spin Qubits**.
Quantum computing technologies

Photonic Circuits

Trapped Ions

Superconducting electronics
A comparison of some of the qubit systems studied so far

<table>
<thead>
<tr>
<th>Qubit system</th>
<th>Decoherence time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^{29}$Si nuclear spins in $^{28}$Si</td>
<td>25 sec</td>
</tr>
<tr>
<td>Spin of trapped ions</td>
<td>15 sec</td>
</tr>
<tr>
<td>Spin of trapped atoms</td>
<td>3 sec</td>
</tr>
<tr>
<td>Nuclear spin (NMR)</td>
<td>2 sec</td>
</tr>
<tr>
<td>Electron spin bound to $^{31}$P</td>
<td>0.6 sec</td>
</tr>
<tr>
<td>NV centre in diamond</td>
<td>2 msec</td>
</tr>
<tr>
<td>Photon polarization</td>
<td>0.1 msec</td>
</tr>
<tr>
<td>Electron spin in QD</td>
<td>3 μsec</td>
</tr>
<tr>
<td>Superconducting Charge/Flux/Phase</td>
<td>4 μsec</td>
</tr>
</tbody>
</table>
Ion-based Qubits

• An ion is an atom stripped of one or more electrons, giving it a positive charge, allowing it to be manipulated by electromagnetic fields.

• The Ion-based scheme uses trapped ions in a very low temperature environment as qubits, where the electronic state of each ion represents the qubit value.

• This can be measured from the photon (particle of light) emitted by the ion.

• For quantum computation, multiple ions can be entangled and this forms a single quantum computing node. University of Oxford has demonstrated the first ‘hybrid’ entanglement between two trapped-ion qubits held in different isotopes of calcium.

• The photons emitted by a node can be used to link and communicate with other nodes, forming a highly scalable networked architecture.

• Ion-based schemes are a mature technology achieving precision rates in excess of 99.9%, which makes them strong candidates to build a quantum computer. A 2 qubit gate is one of the fundamental operations for quantum computing. Currently, Ion-based qubits show the highest accuracy (also called ‘fidelity’) for such operation. The current record of the lowest 2 qubit gate error is ~0.1%.

• Other breakthroughs include near and far-field microwave addressing methods to drive ion-based technology to lower cost.
Ion trap on a microchip for quantum computing set inside a vacuum system in the Oxford Physics Lab
Superconducting Qubits

• In this scheme, special electrical circuits can behave like ‘artificial atoms’.
• These circuits are made from superconducting materials (such as aluminium and niobium), cooled to very low temperatures and operated at microwave frequencies.
• The qubit value can be stored in the number of superconducting electrons (charge qubit), in the direction of a current (flux qubit) or in oscillatory states (phase qubit).
• Qubits can be entangled using microwave photons and the circuit may be linked to other circuits to form a scalable network.
• In addition, superconducting circuits have the advantage of being manufactured using existing integrated circuit fabrication techniques.
• The superconducting qubit landscape has attracted substantial commercial research interest. Both Google and IBM have published results in this area. In March 2015, Google demonstrated a linear array of nine qubits in operation.
Solid-State Spin Qubits

• In this scheme, defects in a material such as diamond or silicon are used as qubits. Solid-state spin qubits have also made significant breakthroughs in the last decade.

• For example, diamond is made up of a regular lattice of carbon atoms. If a carbon atom is missing this forms a vacancy.

• If a nitrogen atom is sitting in the lattice in place of a carbon atom and happens to be next to a vacancy, then this forms a special defect called a ‘nitrogen-vacancy’ (NV) centre.

• The electrons associated with the NV centre have a property called ‘spin’ that describes their magnetic orientation.

• When they subjected to a magnetic field, the electronic spin can be up, down or in a superposition of the two. This then forms a qubit.

• Unlike the previous schemes, NV centres do not require low temperature regimes and are natural light emitters, making the measurement process easier.

• However better manufacturing methods are needed to produce NV centres more reliably and in sufficient number.

• In October 2015, Veldhorst et al. demonstrated the first qubit gate operation on a heavily enriched Silicon platform.

• In 2015, Henson et al. demonstrated entangled single NV qubits separated by more than 1 km using entangled photons 48. This demonstration is an important step towards linking several modular diamond based quantum modules together.
Many countries including Australia, Austria, Canada, China, France, Germany, India, The Netherlands, Japan, Switzerland, Singapore, Spain, USA and the UK have research programmes on Quantum Computing with substantial funding.

For example, since 2002, the Institute for Quantum Computing (IQC) in University of Waterloo, Canada, attracted more than $300 million in investments from the Government of Canada and private investors for pursuing quantum technologies.

Since 2007, Singapore government invested over SG$195 million into quantum technologies, of which quantum computing is a major research area.

In the US, since 2010, the Intelligence Advanced Research Projects Activity (IARPA) invested heavily in several major quantum computing projects, including ‘Coherent Superconducting Qubits (CSQ)’, ‘Logical Qubits (LogiQ)’, ‘Multi-Qubit Coherent Operations (MQCO)’, ‘Quantum Computer Science (QCS)’ and ‘Quantum Enhanced Optimization (QEO)’. Although the amount of investment is not disclosed, from the size of these programmes, the estimated spend is over $200 million.

In 2014, the UK government invested £38 million into a Quantum Computing initiative led by University of Oxford.

In 2015, Intel invested US$50 million into the Dutch consortium for Quantum Technology, QuTech, based in Delft.

Also in 2015, Alibaba has formed a joint venture the Chinese Academy of Sciences, investing $5 million per year for the next 15 years to develop quantum computing.

This is a total of $75 million.

DST has launched the QuIST initiative with a huge response and a clear mandate.
What can Quantum Computers do?

• Analysis suggests that for most problems quantum computers would surpass conventional ones only slightly.

• Is there an efficient quantum algorithm to solve NP-complete problems? Despite much trying, no such algorithm has been found—though not surprisingly, computer scientists cannot prove that it does not exist.

• Quantum computing can be seen as the most stringent test to which quantum mechanics itself has ever been subjected. The most exciting possible outcome of quantum computing research would be to discover a fundamental reason why quantum computers are not possible. Such a failure would overturn our current picture of the physical world, whereas success would merely confirm it.

• If quantum computers ever become a reality, the “killer app” for them will most likely not be code breaking but rather something so obvious it is rarely even mentioned: simulating quantum physics. This is a fundamental problem for chemistry, nanotechnology and other fields, important enough that Nobel Prizes have been awarded even for partial progress.
Where Quantum Computers Fit In

**Example Problems**

- $n \times n$ chess
- $n \times n$ Go
- Box packing
- Map coloring
- Traveling salesman
- $n \times n$ Sudoku
- Graph isomorphism
- Factoring
- Discrete logarithm
- Graph connectivity
- Testing if a number is a prime
- Matchmaking

**Efficiently solved by classical computer**

**Efficiently solved by quantum computer**
“Do quantum computers threaten global encryption systems?”

• The quantum computer that can achieve this feat hasn’t been built yet, and will require on the order of 10 million qubits.

• By that time new encryption schemes will be in place that are resistant even to quantum computers.

• This is termed post quantum cryptography and Google is already implementing it. In July 2016, Google announced it was testing post quantum cryptography on the ‘Chrome Canary’ web browser, using an algorithm they have termed ‘New Hope’
What can be done with Quantum Computers? (1) - Health

• The global healthcare market is estimated to be worth USD $8 trillion.

• Quantum computing is expected to bring the following benefits: accelerate research into diseases such as cancer, find new drugs and pioneer new treatment regimes.

• In **Combating cancer**, QC is expected to bring the following benefits in the long term:
  • Accelerate research into cancer and drug discovery.
  • Improve radiotherapy treatments by calculating the correct dosage and area of exposure to minimize side effects.
  • Revolutionize oncology through individually tailored treatments.

• **Protein folding**
  • Understanding the structure of proteins and how they fold is crucial to developing treatments for misfolded-protein diseases such as Alzheimer’s, Huntington’s, Parkinson’s disease and many cancers.
  • To simulate protein folding is computationally expensive in terms of time and cost, requiring access to supercomputing facilities.
  • The “Folding@home” project from Stanford University relies on volunteers to download special software that runs when their computers aren’t busy. At the time of writing, 87,000 computers around the world are outputting 85,000 teraflops of computing power!
  • Quantum computers are expected to make a huge impact in speeding up these calculations over and above the performance of current supercomputers.
  • In 2012, a team of researchers at Harvard University, led by Professor Alan Aspuru-Guzik, conducted 6 experiments (up to 81 qubits) to apply quantum annealing to lattice protein folding problems using a D-Wave One quantum computer. It was the first time that this technique had been used in the field of biophysics.
What can be done with Quantum Computers? (2) - Finance

- The global market for financial assets (stocks, bonds, securities) is estimated to be $294 trillion, which includes the $69 trillion stock market.

- Some problems in Finance are very difficult to solve with current technology, and can take years of computing time. These include:
  - Dynamic portfolio optimisation.
  - Risk management and regression analysis.
  - Scenario analysis.
  - Quantitative analysis.
  - Option pricing for complex derivatives (which are path dependent). Computing different paths is time consuming and expensive.

- For example, an asset manager who has to rebalance their portfolio to maintain a level of desired asset allocation. Every time this is done, their investors lose money through various costs, termed ‘slippage’.

- With the computational power of quantum computers, the asset manager can decide when to rebalance their portfolio and do this activity less frequently. This has the effect of reducing the impact of high frequency trading on those assets.

- D-Wave and quantum software firm, 1QBit, have teamed up with financial industry experts to create an online community for quantitative analysts, called “Quantum for Quants”. This initiative, launched in May 2016, is to encourage discussion, collaboration, and provide tools and resources for quantum computing.
What can be done with Quantum Computers? (3) - Machine learning

- The purpose of machine learning is to give computers the ability to learn without being explicitly programmed.

- Machine learning is already an increasing feature of our lives even if we are not aware of it. Everyday applications include email filtering, text, speech and facial recognition, targeted advertising and goods (based on viewing or purchase history). More complex examples include artificial intelligence (AI), advanced robotics and driverless cars.

- Quantum machine learning is in its infancy, but ongoing research in algorithm development using the D-Wave quantum computer has already yielded promising results. These include:
  - Very compact and efficient recognizers for low power devices (such as mobiles).
  - Handling highly polluted training data, where a high percentage of the examples are mislabelled. This is very useful for dealing with real-world data.
  - Recognizing objects in images. For example, Google researchers working with D-Wave created a system to answer the question: “Is there a car in this picture?” Over 500,000 optimisation problems were solved during the learning phase.
  - Automatic labelling of news stories and images into categories.
  - Efficient video compression.

- Another example of machine learning is optical character recognition. In 2014, a Chinese research team from the University of Science and Technology of China successfully demonstrated optical character recognition using a 4-qubit quantum processor (based on Nuclear Magnetic Resonance (NMR) technology). The aim of their experiment was to recognize the numbers ‘6’ and ‘9’ written in different handwriting, styles and fonts.
What can be done with Quantum Computers? (4) - Simulation

- **Simulating molecules**
  - The global market for chemicals is estimated to be worth USD 3 trillion, and a number of firms, including Microsoft, have made simulating molecules on a quantum computer as a priority area of research.
  - In July 2016, Google announced it had made an important breakthrough by simulating the Hydrogen molecule for the first time using a scalable quantum device (VQE - Variational Quantum Eigensolver, using superconducting qubits). This is significant because they enable numerically exact prediction of chemical reaction rates, which will advance understanding of chemistry. A conventional computer can also do the modelling but computation times scale up quickly. For example, it takes a supercomputer about 10 days to calculate the energies for propane (C3H8).
  - There are numerous applications in chemistry, for example, making better batteries, finding a better catalyst for carbon sequestration, or producing fertilisers using less intensive methods.
  - A key ingredient in the manufacture of fertilisers is ammonia, which is produced using the intensive ‘Haber Process’. About 450 million tons of fertiliser is made annually, consuming 2% of the world’s energy. If ammonia can be produced more efficiently, it will save costs, bring benefits to the environment, while supporting a growing population. Professor Matthias Troyer at the Institute for Theoretical Physics at ETH Zurich believes that a quantum computer could help design a much more efficient catalyst that will save costs, bring benefits to the environment, while supporting a growing population.

- **Aeroplane wing design**
  - It currently takes several years for engineers to test the design of an aeroplane wing, and model airflow at different angles and speeds.
  - A good design will reduce operating costs, save fuel, which in turn means less carbon emissions. For example, NASA announced a longer, thinner wing design that cuts fuel costs in half.
  - Quantum computers can potentially reduce this process to weeks or months instead of years.
The global market for logistics is estimated to be over $4 trillion, with road freight accounting for $2 trillion.

For a courier company making deliveries, working out the most efficient routes at different times of day can be a complex task. Suppose our driver has to cover for a sick colleague, and has to make deliveries to 4 cities instead of 3. Working out the most efficient route is manageable. However, this problem quickly scales as you add more cities. For example, visiting 10 cities has over 180,000 combinations. Increasing to 15 results in the order of $10^{10}$ combinations! This is known as the ‘Vehicle Routing Problem’ (VRP), and benefits with the computing power and speed-up that quantum computing promises.

Researchers at Manchester Metropolitan University have developed a quantum annealing algorithm for tackling VRP, working with IT technology company ServicePower Technologies PLC, a software provider for logistics firms. In March 2016, ServicePower’s Chief Executive, Marne Martin said: “Quantum annealing is expected to take our scheduling products to the next level, providing the highest in cost reduction to our clients and improving their abilities to provide exceptional services to their own customers.”

ServicePower has made 3 patent applications covering this work.
What can be done with Quantum Computers? (6) - Software Verification & Validation

- Creating highly complex systems such as aircraft, reusable space rockets, or an aircraft carrier requires an enormous amount of effort to verify and validate that every system operates correctly.

- Lockheed Martin is an advanced technologies company, producing elaborate systems for aerospace, defense, space, energy and emerging technologies sectors. Half the costs on creating these solutions is spent on verification and validation.
  - Lockheed Martin turned to D-Wave to see if quantum computing could help identify errors faster. They supplied D-Wave with a sample of a 30-year-old software code from the F-16 jet aircraft. It had taken Lockheed Martin 6 months to find the error, D-Wave found it in 6 weeks.

- Other companies investigating QC for verification and validation is
  - Ford GT car has 10 million lines of software code
  - Boeing 787 Dreamliner 88 has 7 million lines of code.
  - The Windows operating system is on the order of 50 million lines of code.
  - Google’s repository stretches to 2 billion.

- The cost of software glitches can be high. For example, in 2014 car manufacturer Toyota recalled 1.9 million Prius cars globally due to a software error in the hybrid system. In June 2016, another car manufacturer, Fiat, recalled 16,000 Fiat 500e electric cars due to a software fault that would shut down the power in certain situations.

- Quantum computers will allow companies to test their software more thoroughly before customers are affected, saving a fortune in recall costs, preventing lawsuits and public relations disasters.
In 1999, Geordie Rose co-founded D-Wave Systems Inc., the ‘world’s first quantum computing company’, with initial seed capital provided by venture capitalist, Haig Farris. This first commercial investment into quantum computing began with a cheque for $4,059.50 Canadian dollars!

Despite its infancy, confidence in the future of quantum computing is growing. Market Research Media have projected the quantum computing market to exceed USD 5 billion by 2020.

Their quantum annealing machine, the D-Wave 2XTM, has 1,000 qubits, consumes 25 kilowatts of power, and costs in the region of USD 15 million. In 2017, D-Wave shipped its 2,000 qubit processor, which they claim to be 500-1000 times faster than its predecessor.
How slowly is “slowly enough”? On what factors does it depend?

It depends on the so called “eigenvalue gap” i.e. the gap between the smallest and the second smallest eigen-values of the instantaneous Hamiltonian. Problem is that this is exponentially small!
If you think AI is terrifying wait until it has a quantum computer brain

https://thenextweb.com › Artificial Intelligence ▼

Dec 20, 2017 - Rigetti, a quantum computer startup, recently announced its researchers created a method for quantum computers to run a clustering algorithm (a way for AI to separate data into groups). There are a number of companies, including IBM and Google, using AI in the development of quantum systems, but this ...
Thanks
??????