Quantum Computing

Richard Jozsa
Centre for Quantum Information and Foundations
DAMTP
University of Cambridge

Physics and Computation

A key question: *what is computation.. ..fundamentally?*
What makes it work? What determines its limitations?

Information: bits 0,1
two distinguishable states of a **physical** system *"Information is physical"*

Information processing: updating information
A **physical** evolution of the information-carrying physical system

Hence: possibilities and limitations of
information storage / processing / communication
must all depend on the Laws of Physics! (and not mathematics alone!)
Conventional computation (bits / Boolean operations etc.)
is based on the formalism of classical physics.
But classical physics has been superseded by quantum physics …

Benefits of quantum physics

Isn't classical computation already good enough?..

Quantum physics has remarkable theoretical implications for -

Computational power

Quantum algorithms: new kinds of computational steps not available in conventional computing. Exponentially faster algorithms for some computational tasks (not faster clock time but fewer "quantum" computational steps needed to solve the task.)

Communication Quantum states as information carriers, Quantum nonlocality, teleportation.

Information security Quantum cryptography, provably secure against eavesdropping, authentication protocols etc.

Many other technological applications "Nanotechnology" – high precision measurements, sensing, imaging, etc.

Quantum principles and computer science

Classical Information

Bit: 0 or 1 two distinguishable states of a physical system

Quantum Information

Qubit: any quantum physical system with two distinguishable states.
Call them |0> and |1>.

Quantum superposition

For qubits also have **superpositions** **a|0>+b|1>** (with $|a|^2+|b|^2=1$)

State is ***"simultaneously"*** 0 and 1 (in a special sense…)
(gives a new kind of "parallel computation")

Quantum entanglement: single vs. many qubits

(something astonishing happens here!)

Single qubit basic states $|0\rangle$ and $|1\rangle$ and
superpositions $a|0\rangle+b|1\rangle$ (with $|a|^2 + |b|^2 = 1$)

For n qubits: can have superposition of all 2^n n-bit strings
e.g. n=3 we have $a|000\rangle+b|001\rangle+ \ldots + k|111\rangle$ 2^n parameters
But compare to n single qubit states
$(a|0\rangle+b|1\rangle)\ (c|0\rangle+d|1\rangle)\ \ldots\ (p|0\rangle+q|1\rangle)$ only 2n parameters!!
"The whole is greater than the sum of the parts!"

Rich further quantum correlations amongst the separate qubits
("they are entangled") described by the extra parameters.

Quantum entanglement (cont.)

Quantum state description grows *exponentially* with number of qubits!
Corresponding classical growth is only *linear*

e.g. 300 qubits - approx 2^{300} parameters, so a state of 300 qubits can encode a bit string of length 2^{300} (about the total number of atoms in the whole universe!)

 This allows an exponentially enhanced information processing power for quantum over classical computation.

 *But alas there's an issue with reading out the information….*

Quantum measurement

Reading a qubit:

if we measure $a|0\rangle+b|1\rangle$ we see 0 (resp. 1) with probability $|a|^2$ (resp. $|b|^2$) and state is destroyed! – very limiting!

State after measurement is "collapsed" to $|0\rangle$ or $|1\rangle$ according to what was seen, and this collapse is unavoidable!

More formally, any physical process on an n qubit state can extract at most about n classical bits of information about the (exponentially rich) state identity! And any info gain must inflict irreversible disturbance.

☹ Counteracts immediate benefits of superposition and entanglement in computation.

☺ But useful in cryptography – quantum states cannot be cloned (copied) and any attempt at eavesdropping must cause a disturbance that can later be detected.

Putting it all together for a quantum algorithm (intuitively)

Given a function f from n bits to 1 bit (i.e. 2^n values):
(i) Evaluate f on superposition of all inputs $|i_1\, i_2 \ldots\, i_n\rangle$ in n qubits
(needs only one computational run of f)
(ii) Apply quantum operations to very efficiently process this exponentially compressed representation of the whole function.
(iii) Do a quantum measurement: cannot read out much information but it can be (a small amount) of global info about all 2^n values that's hard to get classically (without evaluating lots of f values).

Example: quantum computers are very good at efficiently recognising patterns in data encoded in quantum form.

Shor's quantum algorithm for integer factorisation

Problem of factoring N —number theory (Legendre ~1800)→ Problem of determining the period of a function f (i.e. a pattern feature of its values)

Exponentially faster than any known classical method. Can be used to break RSA and all other public key cryptosystems in current use.

Some further quantum algorithms

Grover's algorithm for search in an unstructured search space
Generally provides polynomial (often quadratic) speedup.
Many applications (find min of unsorted list, pattern matching etc.)

Harrow/Hassidim/Lloyd algorithm for large systems of linear equations
Exponentially faster than classical algorithms.
Applications to finite element numerical methods in engineering, recently machine learning etc.

Quantum algorithm for combinatorial optimisation problems
Uses novel quantum feature provided by quantum adiabatic theorem ("quantum annealing").
Can be applied to any constraint satisfaction problem
Speed-up benefits? – delicate issue.
Used in D-Wave Systems Inc. "quantum machine"

Quantum simulation

Use quantum computer to model/simulate evolution of another quantum system.

Exponential complexity of quantum state description ⇒
e.g. even relatively small molecules (20 atoms?) cannot be adequately modelled on a classical computer.

Many applications: quantum chemistry –
design of new drugs, superconductivity, meta-materials etc.
Can also study biological molecular processes e.g. light harvesting in photosynthesis (solar energy applications) etc.

Likely to be the most important application of quantum computer technology in the near term.

Quantum communication and quantum cryptography

(achievable shorter term goals: uses only small scale quantum processing)

Quantum states of photons: very robust "flying qubits" for quantum communication (in air/daylight or optical fibres).
Then interact with quantum memories to store/process information.
(trapped ions, atoms in optical resonators, colour centres in diamond, quantum dots etc.)

Quantum key distribution

Quantum physics allows provably secure communication
unconditionally secure against any attack allowed by laws of physics

- consequence of quantum measurement disturbance principles.
- impossible to achieve in classical physics.

Has been implemented over a few hundred kilometres.
Devices already commercially available, and much research on range extension (e.g. earth to satellite).

Further crypto applications

Quantum authentication schemes, unforgeable money etc.
Much current research.

Further communication issues

Quantum teleportation: transfer of a quantum state from A to B
"without passing through the space in between"
(in a precise quantum sense)
Exploits nonlocal properties of entangled qubits separated in space.
Proof of principle achieved in labs.
Application to global quantum-safe communication network merging classical and quantum communication ("secure quantum internet").

Further technological applications

High precision sensors (e.g. for gravitational waves etc.),
Extremely accurate atomic clocks,
etc.

From theory ⇒ laboratory ⇒ market place?

Evidence of an imminent revolution in technology

Much progress in past decade for proof of principle,
implementing quantum protocols at level of few qubits.

Several groups have recently announced expectation of having
40-50 controllable clean qubits available within a few years.
(May expect 100 qubits within 5 years?)

Currently many countries investing heavily in quantum information science and technology e.g.
UK (£270million, 5 year programme)
Netherlands (€146million, 10 year programme)
EC (€30million quantERA programme)
Also similar/higher levels in US, China, Japan, Singapore, Australia etc.
April 2016: EC announced intention to fund a €1billion flagship-like initiative on Quantum Technologies.