Quantum Computing and Quantum Information

"The Pleasure of Finding Things Out"

René R. Tol

Classical ---- Quantum

Classical	Quantum
2012: Factoring 193 digits in 30 CPU years (2.2 Ghz)	Factor 193 digits in 0.1 second
Factoring 500 digits in 10^12 CPU years (Age universe estimated 13.7 10^9 years)	Factoring 500 digits in 2 seconds
Mission IMPOSSIBLE	Will probably be done in near future
Note: RSA 2048 => 617 digits Largest present factored RSA (232 digits) took almost 2000 CPU years on 2.2 GHz AMD	

Paralellism, size and energy?

Factoring 2048 bit number (617 digits) ...

- **Classical algorithm:** 10 years run time and requires a server farm covering 1/4 of North America, at cost of $10^6 Trillion. Consumes 10^6 Terawatt (50 times world output 22,000 Tw).

- **Quantum algorithm:** 10K logical qubits and 10M physical (superconducting) qubits. 1cm spacing to allow room for lots of wires. Costs $100B ($10K per physical qubit) and runs 16 hours. Consumes 10MWatt. “We need to get the cost down”

  (source John Martinis)

John Preskill - Introduction to Quantum Information (Part 1) - CSSQI 2012

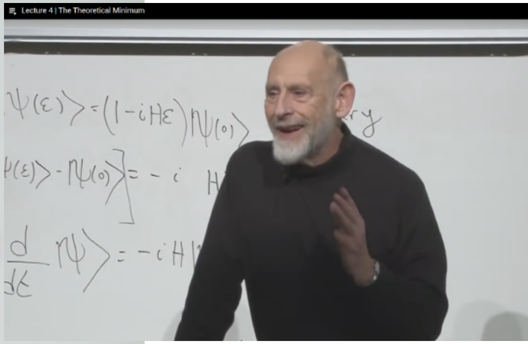
Quantum information vs. Classical information

1) Randomness. Clicks in a Geiger counter are intrinsically random, not pseudorandom. Can't predict outcome even with the most complete possible knowledge of the state.

2) Uncertainty. Operators A and B do not commute means that measuring A influences the outcome of a subsequent measurement of B.

3) Entanglement. The whole is more definite than the parts. Even if we have the complete possible knowledge of the (pure) state of joint system AB, the (mixed) state of A may be highly uncertain.

What T* F*@?



Help Lenny, Help!

The essence of quantum mechanics (draft)

Anything that is physically measurable (an observable) has a corresponding mathematical object, an Hermitian operator. These operators act on quantum states, which are represented by a superposition of orthogonal normalized vectors in a Hilbert space (vector space with inproduct).

A quantum state $|a\rangle$ is called an eigenstate of the operator A (matrix) if the action of the operator on the state returns the same state multiplied by some eigenvalue λ, that is, $A|a\rangle=\lambda|a\rangle$. If the quantum system is in the state $|a\rangle$, then a measurement of the observable A will give the result λ. Note that λ must be a real number (since anything that is physically measurable is a real number).

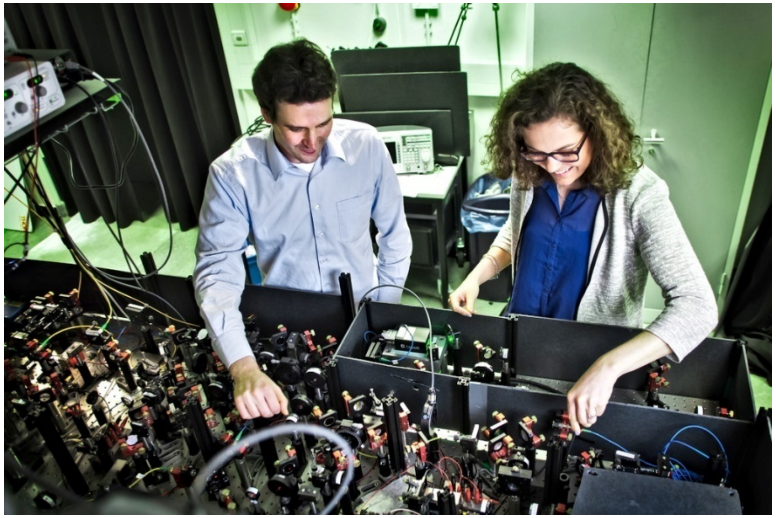
Any system can be described as a superposition of eigenstates:
$|\psi\rangle=\alpha|a\rangle+\beta|b\rangle+\ldots$ (ψ is the wavefunction)
The coefficients α and β, … are called probability amplitudes (complex numbers). The states $|a\rangle,|b\rangle$, .. etc. are eigenstates of A corresponding to eigenvalues λa, λb, … etc.

If we now act on the quantum state $|\psi\rangle$ with A, the result of the measurement will be either λa, with probability $|\alpha|^2$ (the square of the absolute value of the probability amplitude), or λb, with probability $|\beta|^2$. Therefore it is required that $|\alpha|^2+|\beta|^2=1$ so that the total probability sums to 1.

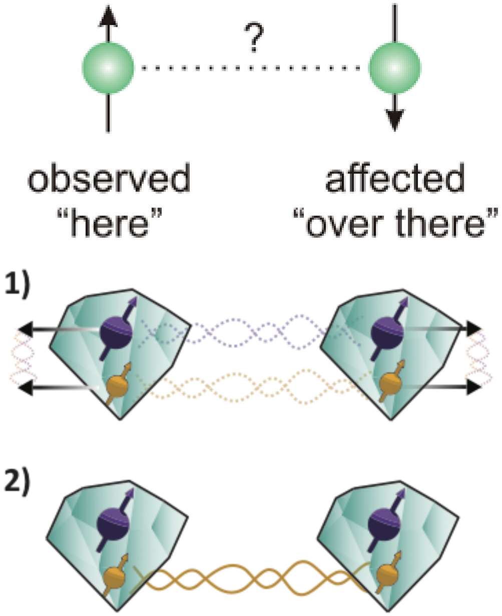
There is no way to know in advance which of the eigenvalues, λa or λb, we will measure; they are "chosen" completely at random when the measurement takes place. We can only predict the probability to measure each of the eigenvalues.

Schrödinger Equation, evolution of a system in time (H is Hamiltonian): $H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$

Entanglement: Quantum communication



Tim Taminiau en Julia Cramer in QuTech-lab, Delft, the Netherlands



Ronald Hanson, Leo Kouwenhoven et. al.: "Quantum networks have the potential to reach metropolitan scales in the near term, opening up new challenges due to the time required to signal successful entanglement generation between nodes separated by many kilometers. Nitrogen-vacancy centres in diamond are promising candidates for the nodes of such a network, combining an electronic spin broker qubit interface for entanglement generation and local processing with long lived 13C nuclear-spin memory qubits."

Links and References

- http://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one
- timeline Qc.jpg
- https://newscientist.nl/dossiers/quantumcomputer/
- https://www.research.ibm.com/ibm-q/learn/what-is-ibm-q/
- https://www.quantiki.org/
- http://www.yuj.nl/yuj-advies

Reality?

"This Statement is False"

Is this statement True…. or…. False?

"The opposite of a fact is falsehood, but the opposite of one profound truth may very well be another profound truth." Niels Bohr

Discussion

ShivaNataRaja at CERN, Geneva

René R. Tol
Yuj Advies
Rene.Tol@yuj-nl
+31 6 46 220 200