Quantum Information and Computation

January 22, 2018

Contents

0 Miscellaneous

All course materials downloadable from *http* : *//www.qi.damtp.cam.ac.uk/node/*272.

Some foci of the course: why do we need *quantum* computation and informatoin? What is information? Classical information is presented by bits – boolean variable with values 0,1, and bit strings for more alternative messages. Also, what is computation? In the classical sense it is updating bit strings by prescribed sequence of steps called "program". It uses basic elementary Boolean operatons/gates, e.g. AND, OR, NOT, SWAP acting on 1 or 2 bits.

Now if information consists of bits, then what is a bit? It is not abstract maths but two distinguishable state of a physical system.

Computation (info processing) must correspond to a physical evolution of the system representing the bits. So possibilities if info storage/communicating/processing must all rest on laws of physics and cannot be determined by abstract thought/mathematics alone.

Some benefits/issues of quantum vs classical physics:
(a) Computing power (computational complexity). A quantum computer cannot compute anything that's not computatble *in principle* on a classical computer. However, computational hardness, or amount of resources needed, matters. If it's too high then the problem is uncomputable *in practice*.

Example. Task: given an integer N ($n = O(\log N)$ digits), we have an input size n. We wish to find a polynomial time algorithm, which runs in number of steps bounded by polynomials in n. Such an algorithm is feasible in practice. Algorithms needing exponential time are not feasible in practice, for example, trial division, whch requires $O(\sqrt{N}) = O(2^{n/2})$ steps. The best known classifical factoring algorthm runs in $2^{O(n^{1/3}(\log n)^{1/3})}$ which is not feasible. However, there is a quantum algorithm (Shor's Algorithm) that runs in polynomial time, and is in fact only $O(n^3)$.

(b) Communication/security benefits:
• Provably secure communication pososible with quantum effects, which is impossible classically;
• Novel kinds of communicator, e.g. quantum teleportation, etc.

(c) Technological issues: Moore's law: miniaturisation of classicl computing components (since 1965, factor of 4 every 3.5 years). Now at atomic scale where classical physics fails!

However, building a quantum computer seems to be very difficult now, and is beyond human's capability at this point. In 2018 (this year) we expect to have a working quantum computer of size 50 qubits.

Principles of Quantum Mechanics and Dual bra-ket notation.

Bra & ket vectors:

Let V be a finite dimensional complex vector space, with inner product. Vectors are written as $|v\rangle$ (rather than $\mathbf{v}$). This is called the *ket vectors* or just *kets*; often work in $2-$dimensional V_2 with chosen orthonormal basis $\{|0>, |1\rangle\}$ labelled by bit values $0, 1$.