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.

1 Principles of Quantum Mechanics, Dual bra-ket notation

1.1 Bra and 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 $0, 1$; kets always written in components as column vectors, i.e.

$$|v\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, a, b \in \mathbb{C}$$

We call the conjugate transpose, $|v\rangle^+$ a *bra vector*, written with "mirror image notation",

$$\langle v| = |v\rangle^+ = a^*\langle 0| + b^*\langle 1| = (a^* \ b^*)$$

so *row vectors* in components.

If $|w\rangle = c|0\rangle + d|1\rangle$ is another ket. Inner product of $|v\rangle$ with $|w\rangle$ written by juxtaposing $|v\rangle^+$ with $|w\rangle$,

$$\langle v|w\rangle = |v\rangle^+|w\rangle = (a^*b^*)\begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d$$

which is the usual hermitian inner product on $\mathbb{C}^2$.

cf common math notaiton for inner product, $\langle \mathbf{v}, \mathbf{w} \rangle$.

$V \otimes W$ has dimension mn with orthonormal basis $\{|e_i\rangle \otimes |f_j\rangle\}_{i,j}$. General ket on $V \otimes W$ is

$$|\xi\rangle = \sum c_{ij}|e_i\rangle \otimes |f_j\rangle$$

We have a natural bilinear map $f : V \times W \to V \otimes W$. If $|\alpha\rangle = \sum a_i|e_i\rangle$, $|\beta\rangle = \sum b_j|f_j\rangle$, then

$$\begin{aligned}(|\alpha\rangle, |\beta\rangle) \xrightarrow{f} |\alpha\rangle \otimes |\beta\rangle &= (\sum a_i|a\rangle) \otimes (\sum b_j|f_j\rangle) \\ &= \sum_{i,j} a_ib_j|e_i\rangle \otimes f_j\rangle\end{aligned}$$

In components, $|\alpha\rangle \sim a_i$'s, $|\beta\rangle \sim b_j$'s, $|\alpha\rangle \otimes |\beta\rangle \sim a_ib_j$. Note that $\otimes$ is not commutative: in general $|\alpha\rangle \otimes |\beta\rangle \neq |\beta\rangle \otimes |\alpha\rangle$ even if $V = W$.

We often omit the $\otimes$ symbol, i.e. we write $|\alpha\rangle \otimes |\beta\rangle$ as $|\alpha\rangle|\beta\rangle$.

1.2 Product vectors and entangled vectors

Any vector $|\xi\rangle \in V \otimes W$ of form $|\xi\rangle = |\alpha\rangle|\beta\rangle$ (for $|\alpha\rangle \in V, |\beta\rangle \in W$), called a *product vector*.

This is *not* surjective; any $|\xi\rangle \in V \otimes W$ that is *not* a product vectors is called *entangled.*

We will mostly be concerned with tensor products of V_2 with itself, write K-fold tensor product as $\otimes^k V_2 = \underbrace{V_2 \otimes ... \otimes V_2}_{k\ times}$. This has dimension 2^k, and orthonormal basis $|i_1\rangle \otimes ... \otimes i_k\rangle$, $i_1, ..., i_k = 0\&1$ labelled by k-bit strings. We often write $|i_1\rangle \otimes ... \otimes |i_k\rangle$ as $|i_1\rangle|i_2\rangle...|i_k\rangle$ or $|i_1 i_2 ... i_k\rangle$, a k-bit substring.

Example. $|v\rangle = |00\rangle + |11\rangle \in V_2 \otimes V_2 = \otimes^* V_2$ is entangles. To see this, suppose $|v\rangle = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$ for some $a, b, c, d..$ Now $RHS = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$. Comparing coefficients with $|v\rangle$, $ac = 1, ad = 0, bc = 0, bd = 1$ contradiction since we can get both $abcd = 1$ and $abcd = 0$.

We can show (sheet 1) that for any $|v\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \sum c_{ij}|i\rangle|j\rangle$, where $c_{ij} = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$. $|v\rangle$ is entangled iff $\alpha\delta - \beta\gamma \neq 0$.
Note that this iff holds only in 2-dimensions.

For general dimensions $V_n \otimes V_n$, any ket $\sum_{i,j=0}^{n-1} A_{ij}|i\rangle|j\rangle$ is product vector iff $[A_{ij}]$ matrix has rank 1, so $\det A = 0$ is necessary but *not sufficient.*

1.3 Inner product on $V \otimes W$

This is induced by the inner products on V and W. For product vectors, inner product of $|\alpha_1\rangle|\beta_1\rangle$ with $|\alpha_2\rangle|\beta_2\rangle$ is ('matching slots')

$$(\langle\beta_1|\langle\alpha_1|)(|\alpha_2\rangle|\beta_2\rangle) = \langle\alpha_1|\alpha_2\rangle\langle\beta_1|\beta_2\rangle$$

and extend by linearity to general vectors ($(AB)^+ = B^+A^+$)(?).

Note notation: The bra vector of $|\alpha\rangle|\beta\rangle$ is often written in reverse order $\langle\beta|\langle\alpha|$. It's always important to keep track of component spaces.

Sometimes to be explained we label slots, eg write $|\alpha\rangle_A|\beta\rangle_B$ with bra ${}_A\langle\beta|_B\langle\alpha|$.

Quantum principle (QM1) (physical staets): states of any (isolated) physical system S are represented by unit vectors in a complex vector space V with innter product.

The simplest non-trivial case $V = V_2$, 2-dimensional: choose a pair of orthonormal vectors, label them with bit values.
viz (?) $|0\rangle$ and $|1\rangle$, called *computational basis* or *standard basis.*

General staet: $|\psi\rangle = a|0\rangle + b|1\rangle$, $\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$.

We say $|\psi\rangle$ is a *superposition* of states $|0\rangle$ and $|1\rangle$, with *amplitude* a and b respectively.

Qubit: any quantum system with 2-dimensional state space with a choice of orthonormal basis.

Conjugate basis (or X-basis): given $0\rangle$, $|1\rangle$, we define

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

(QM2) (composite systems)
If systems S_1 has staet space V_1, S_2 has state space V_2, then joint system $S_1 S_2$ has state space $V_1 \otimes V_2$.