Quantum Information and Computation

January 26, 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

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

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 states): states of any (isolated) physical system S are represented by unit vectors in a complex vector space V with inner 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 state: $|\psi\rangle = a|0\rangle + b|1\rangle$, $\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$.

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 state space V_1, S_2 has state space V_2, then joint system $S_1 S_2$ has state space $V_1 \otimes V_2$.

Example. n qubits have state space $V_2^{\oplus n}$ which has dimension 2^n.
• n qubit state (ψ): called *product state* if $|\psi\rangle = |v_1\rangle |v_2\rangle ... |v_n\rangle$. It is entangled otherwise.
• Computaitonal or standard basis: we write

$$|i_1\rangle |i_2\rangle ... |i_n\rangle := i_1 i_2 ... i_n\rangle$$

where $i_1, ..., i_n = 0, 1$; here we have 2^n orthonormal states.

Note (!) as number n of qubits grows linearrly, full state description (eg amplitudes $|\psi\rangle = \sum \langle i_1 i_2 ... i_n | i_1 i_2 ... i_n \rangle$) grows exponentially. In contrast, in the classical case, state space of $S_1 S_2$ is a *Cartesian product*, so if S needs K parameters, then $\underbrace{SS...S}_{n \text{ times}}$ has only nK parameters.

1.4   Diract notation on linear maps

Consider linear maps on V_2: suppose $|v\rangle = a|0\rangle + b|1\rangle$, $|w\rangle = c|0\rangle + d|1\rangle$. Then the *ket-bra product* gives

$$M = |v \times w| = \begin{pmatrix} a \\ b \end{pmatrix} (c^* \ d^*) = \begin{pmatrix} ac^* & ad^* \\ bc^* & bc^* \end{pmatrix} \ (*)$$

a linear map on V_2 (for any $|x\rangle = x_0|0\rangle + x_1|1\rangle$):

$$M|x\rangle = (|v \times w|)|x\rangle = |v\rangle(\langle w|x\rangle) = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix} = \begin{pmatrix} ac^* x_0 + ad^* x_1 \\ bc^* x_0 + bd^* x_1 \end{pmatrix}$$

this is a rank-1 map, with kernel being all $|x\rangle$'s $\perp |w\rangle$, i.e. $\langle w|x\rangle = 0$.

For general linear map $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, note first that the ket-bra products for $|0\rangle \mid |1\rangle$ basis vectors,

$$|0 \times 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (10) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$|0 \times 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$|1 \times 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$$|1 \times 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

so $A = a|0 \times 0| + b|0 \times 1| + c|1 \times 0| + d|1 \times 1|$.

Note $\langle w|v \rangle = \text{tr}(|v \times w|)$ from (*) as cyclic property of trace.

Projection operators:

Important special case of ket-bra product (*) if when $|v\rangle = |w\rangle$, if $|v\rangle$ normalised ($\langle v|v \rangle = 1$), then $\Pi_v = |v \times v|$ is operator of projection into 1-dimensional subspace spanned by $|v\rangle$. For example, we have

$$\Pi_v \Pi_v = |v \times v||v \times v| = |v\rangle\langle v|v\rangle\langle v| = |v \times v| = \Pi_v$$

Also we have $\Pi_v|a\rangle = 0$("$=|v\rangle\langle v|a\rangle$") if $|a\rangle \perp |v\rangle$, i.e. $\langle v|a\rangle = 0$.

More generally, if E is any d-dimensional linear subspace of an n-dimensional V and $\{|e_1\rangle, ..., |e_d\rangle\}$ any orthonormal basis of E, then $\Pi_E = |e_1 \times e_1| + ... + |e_d \times e_d|$ is operator of projection into E. Note that being orthonormal means that $\langle e_i|e_j\rangle = \delta_{ij}$.

1.5 Tensor products of maps

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ are linear maps on V_2, then $A \otimes B : V_2 \otimes V_2 \to V_2 \otimes V_2$ defined by action on basis $|i\rangle|j\rangle$, $i, j = 0, 1$4:

$$|i\rangle|j\rangle \xrightarrow{A \otimes B} (A|i\rangle) \otimes (B|j\rangle)$$

(on product states, $|v\rangle|w\rangle \to (A|v\rangle) \otimes (B|w\rangle)$).

It's easy to check matrix of $A \otimes B$ is given by the block structure

$$(A \otimes B) = \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix}$$

Important special cases are $I \otimes A$ and $A \otimes I$.

(QM3) (Physical evolution of quantum systems)
Any physical (finite time) evolution of a quantum system is represented by a *unitary* operation on the state space.

Recall: U is unitary iff $U^{-1} = U^+$ iff U maps an orthonormal basis to an orthonormal set of vectors iff the columns (rows) of the matrix of U are an orthonormal set of vectors.

Partial inner products for vectors in $V \otimes W$: Any ket $|v\rangle \in V$ defines a linear map $V \otimes W \to W$ called "partial IP on V" defined on basis vectors $|e_i\rangle \oplus |f_j\rangle$:

$$|e_j\rangle|f_j\rangle \to \langle v|e_i\rangle|f_j\rangle$$

and extend by linearity. Similarly, for $|w\rangle \in W$ we have a partial IP on W: $V \otimes W \to V$.

Example. For $V = V_2 = W$, i.e. 2 qubits, we have

$$|\xi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \in V \otimes V$$

can form partial IP with $|0\rangle$ on either slot. To keep track of "slots", when spaces are equal we will first label the slots A and B: for $|\xi\rangle = a|00\rangle_{AB} + ...$, we label $|0\rangle_A|0\rangle_B$.

Orthonormal relations $\langle i|j\rangle = \delta_{ij}$ gives partial IP on A slot,

$$_A\langle 0|\xi\rangle_{AB} = a_A\langle 0|0\rangle_A|0\rangle_B + ... + d_A\langle 0|1\rangle_a|1\rangle_B$$
$$= a|0\rangle_B + b|1\rangle_B$$

"pick out terms of $|\xi\rangle_{AB}$ with $|0\rangle$ in A-slot.

Similarly

$$_B\langle 0|\xi\rangle_{AB} = a|0\rangle_{AB}\langle 0|0\rangle_B + c|1\rangle_{AB}\langle 0|0\rangle_B$$

(QM4) Quantum measurements and Born rule.

Suppose we are given a single instance of a quantum state $|\psi\rangle$ of physical system, state space V, dimension n. Let $\mathcal{B} = \{|e_1\rangle, ..., |e_n\rangle\}$ be any orthonormal basis of V. We can measure $|\psi\rangle$ relative to basis $\mathcal{B}$. Possible outcomes $j = 1, 2, ..., n$, $Prob(j) = |\langle e_j|\psi\rangle|^2 = |a_j|^2$ if $|\psi\rangle = \sum_{j=1}^n a_j|e_j\rangle$. If outcome j is seen, then after the measurement state is no longer $|\psi\rangle$, but it has been "collapse" to $\psi_j\rangle = |e_j\rangle$. So repeated measurement gives *same* result j with certainty.

This is called a *complete projective* (or von Neumann) measurement: "complete" refers to *one*-dimensionality of orthogonal subspaces defined by $|e_j\rangle$'s.

Incomplete projective measurements:

Let $\{E_1, E_2, ..., E_d\}$ be decomposition of V into d mutually orthogonal subspaces, so $V = E_1 \oplus ... \oplus E_d$. Let Π_i be projection into E_i. Then the incomplete measurement of $|\psi\rangle$ w.r.t. this orthogonal decomposition is the following quantum operation.

The possible outcomes are $j = 1, 2, ..., d$. Now $Prob(j)$ is the squared length of projection of $|\psi\rangle$ into E_j, and is then equal to $\langle\psi|\Pi_j^+\Pi_j|\psi\rangle = \langle\psi|\Pi_j|\psi\rangle$ since $\Pi_j^+ = \Pi_j$ and $\Pi_j\Pi_j = \Pi_j$ for any projection operator.

The post-measurement staet is the projected ("collapsed") vector re-normalised $|\psi_j\rangle = \Pi_j|\psi\rangle/\sqrt{prob(j)}$.

Example. Parity measuremnt:

Parity of 2-bit string b_1b_2 is the mod-2 sum $b_1 \oplus b_2$, i.e. the number of 1's mod 2.

Parity measurement on 2 qubits is the incomplete measurement relative to the orthogonal decomposition $E_0 = span\{|00\rangle, |11\rangle\}$, $E_1 = span\{|01\rangle, |10\rangle\}$.

For $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, we get outcome 0 with probaility $|a|^2 + |d|^2$, and post-measurement state would be $(a|00\rangle + d|11\rangle)/\sqrt{|a|^2 + |d|^2}$.

Measurement of "quantum observables" (as in most textbook):

Quantum observable θ is Hermitian operator on V. So θ has real eigenvalues

$\lambda_j, j = 1, ..., d$. Eigenspaces Λ_j mutually orthogonal, $\dim(\Lambda_j) =$ multiplicity of λ_j, $V = \Lambda_1 \oplus ... \oplus \Lambda_d$.

'Measurement of quantum observable θ' is then just the (generally incomplete) measurement relative to this orthogonal decomposition, except outcomes now labelled by eigenvalues λ_j (not just labels j).

λ_j values often have further physical significance (energy, spin etc), and have e.g. average value equal to $\sum_j \lambda_j prob(\lambda_j)$. But for purposes of providing information about $|\psi\rangle$, choice of *labelling* of outcomes is immaterial.

Extended Born rule:

special case of an incomplete measurement. Measuring a component part of a composite system.

Suppose $|\psi\rangle$ is state of composite system $S_1 S_2$, with staet space $V \otimes W$.

Let $\mathcal{B}_V = \{|e_1\rangle, ..., |e_n\rangle\}$ be an orthonormal basi of V. $|\psi\rangle$ can be uniquely expanded as

$$|\psi\rangle_{VW} = \sum_i |e_i\rangle_V |\xi_i\rangle_W$$

where $|\xi_i\rangle$'s generally neither normalised nor orthogonal. We have $\langle\psi|\psi\rangle = \sum_i \langle\xi_i|\xi_i\rangle = 1$. In fact (sinice $|G\rangle$ orthonormal), we have $|\xi_i\rangle_W = \langle e_i|\psi\rangle_{VW}$. Now we can perform a measurement of $|\psi\rangle$ relative to basis $\mathcal{B}_V$ of V. This is the incompplete measurement on $V \otimes W$ with outcomes $i = 1, 2, ..., n$, and corresponding orthogonal subspaces $E_i = span(|e_i\rangle \otimes |\xi\rangle$; any $|xi\rangle \in W)$, $\dim(E_i) = \dim(W)$. Corresponding projectors are

$\Pi_i = |e_i \times e_i| \otimes I_W$, so we get $prob(i) = \langle\xi_i|\xi_i\rangle$. Post-measurement state for i is

$$|\psi_i\rangle = |e_i\rangle|\xi_i\rangle / \sqrt{\langle\xi_i|\xi_i\rangle}$$

"just pick out terms of $|\psi\rangle$ with $|e_i\rangle$ in V-slot".