QUANTUM INFORMATION AND COMPUTATION
EXERCISE SHEET 1

Nilanjana Datta n.datta@damtp.cam.ac.uk (Lent 2024-2025)

(1) (Basic entanglement for two qubits)
(a) Show that the state $|A_k\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + (-1)^k |11\rangle)$ is entangled if $k = 1$ and unentangled if $k = 0$. Express the latter case explicitly as a product state.

(b) Can $|A_k\rangle$ for $k = 0$ or 1 be prepared from $|0\rangle |0\rangle$ by applying only 1-qubit gates to the qubits? Give a reason for your answer.

(c) Generalising (a), show that $|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle$ is entangled iff $\alpha\delta - \beta\gamma \neq 0$.

(2) (Born rule, Pauli operations)
Let $|\psi\rangle = a |0\rangle + b |1\rangle$ be any 1-qubit quantum state. Suppose we receive one of the four states $|\psi\rangle$, $X |\psi\rangle$, $Y |\psi\rangle$, and $Z |\psi\rangle$, with equal prior probabilities of 1/4. (We could equivalently use instead the four Pauli operations I, σ_x, σ_y and σ_z, and the action on $|\psi\rangle$ is called Pauli-twirling.)

Show that any outcome of any complete projective measurement on the Pauli-twirled version of $|\psi\rangle$ has probability half. (Thus the received state contains no information at all about the identity of $|\psi\rangle$.)

(3) (Born rule, no-signalling, but having nonlocality)
Consider the 2-qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Suppose that the two qubits are separated widely in space and held by Alice (A) and Bob (B) respectively, who can then apply only local quantum operations i.e. unitary gates and measurements only to the qubit they hold. Introduce the 1-qubit gate ("rotation by θ")

$$U(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

(a) Suppose A applies $U(\alpha)$ and B applies $U(\beta)$. Show that the resulting state is

$$|\psi_{\alpha\beta}\rangle = \frac{1}{\sqrt{2}} \left(\cos(\alpha-\beta) |00\rangle - \sin(\alpha-\beta) |01\rangle + \sin(\alpha-\beta) |10\rangle + \cos(\alpha-\beta) |11\rangle\right).$$

Deduce that for any choice of α and β, if we measure either one of the qubits of $|\psi_{\alpha\beta}\rangle$ in the computational basis we will get output 0 or 1 with equal probabilities of half. Show that this remains true even if the other party has (unbeknown to us) already made the measurement and obtained his/her suitably random outcome and post-measurement state i.e. choice of local angle on one side cannot affect the measurement statistics obtained locally on the other side. (This is another example of the no-signalling principle, discussed in lectures.)

(b) Suppose A and B now both measure (in the computational basis) their held qubit of $|\psi_{\alpha\beta}\rangle$ (in either order or simultaneously – the statistics are the same). Show that for the two bit outcome obtained from the two local measurements, prob(outcomes differ) $= \sin^2(\alpha - \beta)$.

(c) (Optional, but interesting! Good for discussion if time permits)
We now consider only three angle settings $\theta = -\frac{\pi}{6}, 0, \frac{\pi}{6}$. Let $M_A(\alpha)$ denote the following operation for Alice: apply $U(\alpha)$ to her qubit and measure it in the computational basis. Similarly $M_B(\beta)$ for Bob. Consider now the following experiment denoted $E(\alpha, \beta)$: A and B have many $|\psi\rangle$ states and perform a long sequence of $M_A(\alpha)$ and $M_B(\beta)$ with each choosing one of the allowed angles (which is kept the same for the whole sequence). We imagine that for each $|\psi\rangle$ the local operations are done essentially simultaneously (or at least at a spacelike interval). For long sequences, probabilities will be reflected in frequencies of occurrence of 0's and 1's. Show

that the following statistics will be seen:

(i) $E(0,0)$:	prob(differ) $= 0$	A and B's sequences will be the same sequence.
(ii) $E(0,-\frac{\pi}{6})$:	prob(differ) $= 1/4$	The sequences will differ in about 1 in 4 places.
(iii) $E(\frac{\pi}{6},0)$:	prob(differ) $= 1/4$	The sequences will differ in about 1 in 4 places.
(iv) $E(\frac{\pi}{6},-\frac{\pi}{6})$:	prob(differ) $= 3/4$	The sequences will differ in about 3 in 4 places!

Recall that the sequence seen locally by A or B will, in every case, be uniformly random, in contrast to the angle-dependent *correlations* above.

Although we cannot apply two different $M(\theta)$ operations on any single system (for two different angles) on one side, we can still consider counterfactually the sequences of outcomes that *would* have been obtained *if* A or B had performed each of the three possible actions on their side for any choice on the other side.

By considering these sequences and the correlations between them implied by (i) to (iv) above, argue that it is impossible for the local outcomes at A (resp. B) to be independent of the choice of angle chosen and used remotely at B (resp. A) i.e. that the local outcomes at A (resp. B) must be "instantaneously influenced" by the choice of angle at B (resp. A).
[Suggestion: Get Alice and Bob to do $E(\frac{\pi}{6},-\frac{\pi}{6})$, and ask each of them (separately) to think about what *would* have happened *if* the other party had used a different angle.]

Stated more colourfully, we see that the correlations in the quantum measurement outcomes can only occur if there is some "spooky action at a distance" (Einstein's phrase) implied by the quantum rules for local operations on composite systems. Note also that by (a), although the "instantaneous influence" must exist, it cannot be used to instantaneously send a signal from A to B (or vice versa) by suitable choice of local angle, since the effect is manifest only in *correlations* (which require the local outcomes from both sides to be compared, to be noticed) and not in any *local* measurement statistics separately.

(4) (Schmidt form; making 2-qubit states)
The Schmidt decomposition theorem for bipartite quantum states is the following:
Theorem: Let $|\psi\rangle_{AB}$ be any quantum state of a composite system comprising an m dimensional system A and n dimensional system B. Let $d = \min\{m, n\}$.
Then there are orthonormal bases $\{|\alpha_1\rangle, \ldots, |\alpha_m\rangle\}$ of A and $\{|\beta_1\rangle, \ldots, |\beta_n\rangle\}$ of B (called *Schmidt bases* for $|\psi\rangle$) and non-negative real numbers $\lambda_1, \ldots, \lambda_d$ (called the *Schmidt coefficients* of $|\psi\rangle$), such that

$$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |\alpha_i\rangle |\beta_i\rangle$$

i.e. when expressed in the Schmidt bases, $|\psi\rangle$ has no cross terms $|\alpha_i\rangle |\beta_j\rangle$ for $i \neq j$.
The number of non-zero Schmidt coefficients is called the *Schmidt rank* of $|\psi\rangle$. $\square$

We will consider the Schmidt decomposition of states of two qubits (i.e. $m = n = 2$).

(a) By inspection (or otherwise) find Schmidt bases, coefficients and ranks for the product state $|a\rangle |b\rangle$ and for $|A_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$.
Show that $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$ and deduce that Schmidt bases are not uniquely determined if two Schmidt coefficients are equal.

(b) Recall the statement of the singular value decomposition theorem for matrices (or google it if you don't know it). Here we'll use it for 2×2 matrices. Writing a general 2-qubit state as $|\psi\rangle = \sum_{ij} a_{ij} |ij\rangle$ use the singular value decomposition theorem to prove Schmidt decomposition theorem for pairs of qubits.
[Note that the Schmidt form for higher dimensions follows similarly from the singular value decomposition theorem for larger matrices.]

(c) Let $\{|\alpha_0\rangle = a|0\rangle + b|1\rangle, |\alpha_1\rangle = c|0\rangle + d|1\rangle\}$ be any orthonormal basis for a qubit. Show that there is a 1-qubit unitary gate U with $U|0\rangle = |\alpha_0\rangle$ and $U|1\rangle = |\alpha_1\rangle$.
Hence or otherwise, show that any 2-qubit state can be manufactured from $|0\rangle|0\rangle$ by application of a sequence of unitary gates comprising only 1-qubit gates and at most just a *single* application of the 2-qubit CX gate. For which states is the CX gate not required?

(d) (optional, if time permits.) The Schmidt form does *not* in fact generalise to *tri*-partite systems. To see this, show that there are states $|\psi\rangle_{ABC}$ of three qubits that cannot be expressed as

$$|\psi\rangle = \sum_{i=1}^{2} \lambda_i |\alpha_i\rangle |\beta_i\rangle |\gamma_i\rangle$$

(i.e. with no cross terms in the bases) for any triple of bases $\{|\alpha_i\rangle\}, \{|\beta_i\rangle\}, \{|\gamma_i\rangle\}$. You may assume that Schmidt bases are unique (up to overall phases and ordering of vectors) if the Schmidt coefficients are different. It may be helpful to begin with the (valid) Schmidt form of $|\psi\rangle_{ABC}$ for the *bi*-partition of A vs. BC.

(5) (No-cloning)
(a) Let $|\xi_i\rangle$ and $|\eta_i\rangle$ for $i = 0, 1$ be two pairs of states. Show that if $\langle\xi_0|\xi_1\rangle = \langle\eta_0|\eta_1\rangle$ then there is a unitary U with $U|\xi_i\rangle = |\eta_i\rangle$ for $i = 0, 1$. (Note: this is a generalisation of the first part of question 4(c)).

(b) (a stronger no-cloning theorem) Consider the problem of cloning for two distinct non-orthogonal states $|\alpha_i\rangle$ with $i = 0, 1$. We know that cloning is impossible but suppose that in addition to the instance of $|\alpha_i\rangle$ we are also given some extra (generally quantum) information about it, in the form of a state $|\beta_i\rangle$ (generally depending on i).

Write down the general form of a unitary process that corresponds to the cloning of $|\alpha_i\rangle$ with the assistance of $|\beta_i\rangle$. By mimicking the proof of the no-cloning theorem in lectures, show that if we are given $|\alpha_i\rangle|\beta_i\rangle$ then it is still impossible by any unitary process to obtain a second copy of $|\alpha_i\rangle$, unless $|\alpha_i\rangle$ can already be created from $|\beta_i\rangle$ *alone* i.e. the extra assistance state must already contain the *full* information of $|\alpha_i\rangle$ within itself.

(6) (No-deleting principle) (a kind of "opposite process" to cloning)
A *deleting operation* for the states $|\alpha_i\rangle$ (as in question (5)(b)) is any process acting on two copies $|\alpha_i\rangle|\alpha_i\rangle$ with an ancilla, effecting the following:

$$|\alpha_i\rangle |\alpha_i\rangle |M\rangle \to |\alpha_i\rangle |0\rangle |M_i\rangle$$

i.e. given two copies we 'delete' one of them. Here $|0\rangle$ is any fixed state (independent of i) and $|M_i\rangle$ is a state that can depend on i.

(a) Show that if such a deleting operation is unitary then $|\alpha_i\rangle$ can always be reconstituted from $|M_i\rangle$ alone i.e there is a unitary operation U with $U|0\rangle|M_i\rangle = |\alpha_i\rangle|N\rangle$ where $|N\rangle$ is independent of i. In this sense, quantum information cannot be deleted by a unitary process, even if we are given a second copy to help delete it; it can only be moved out to 'another place' ("the rubbish bin") from where it can always be perfectly retrieved.

(b) Show that quantum information can be deleted if we allow measurements in the process.

(c) Can *classical* information be deleted by purely reversible Boolean operations (given, as above, a second copy initially to help)?

(7) (Unambiguous state discrimination)
Consider the states

$$\begin{aligned} |\psi_0\rangle &= \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |\psi_1\rangle &= \cos\theta\,|0\rangle - \sin\theta\,|1\rangle \end{aligned}$$

with $0 \leq \theta \leq \pi/4$.

(a) Consider the 2-qubit linear operation U_α defined by

$$\begin{aligned} U_\alpha\,|00\rangle &= \cos\alpha\,|00\rangle + \sin\alpha\,|11\rangle \\ U_\alpha\,|11\rangle &= \sin\alpha\,|00\rangle - \cos\alpha\,|11\rangle \\ U_\alpha\,|01\rangle &= |01\rangle \qquad U_\alpha\,|10\rangle = |10\rangle\,. \end{aligned}$$

Show that U_α is unitary. Let $|\xi_i\rangle = U_\alpha\,|0\rangle\,|\psi_i\rangle$. Find α such that $|\xi_0\rangle$ and $|\xi_1\rangle$ have orthogonal projections into the 2-dimensional subspace spanned by $|00\rangle$ and $|01\rangle$.

(b) Using the result of (a), construct a scheme for the unambiguous discrimination of the states $|\psi_i\rangle$ i.e. a quantum process with three outputs called 0, 1 and 'fail', such that if 0 (resp. 1) is obtained then the state was certainly $|\psi_0\rangle$ (resp. $|\psi_1\rangle$), and if 'fail' occurs then all information about the state has been lost (and we cannot do anything further to discriminate them). Show that the probability of failure is $|\langle\psi_0|\psi_1\rangle|$.

(c) What should we do if $\pi/4 \leq \theta \leq \pi/2$? Can we still unambiguously discriminate the states?

(8) (More on unambiguous discrimination)
Let $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle\}$ be a set of n quantum states. They can be unambiguously discriminated if there is a quantum process with $n+1$ outcomes labelled $1, \ldots, n$ and 'fail' such that if the outcome k occurs then the input state was certainly $|\alpha_k\rangle$, and if outcome 'fail' occurs then the process was inconclusive. Also for every k, on input $|\alpha_k\rangle$, outcome k must have a *non-zero* probability of occurring.

You may assume that any prospective discrimination process is a unitary process (with inclusions of ancillas) having just a final measurement at the end (in fact without loss of generality – cf Remark in lecture notes after the statement of the no-cloning theorem).

(a) Show that if the states can be unambiguously discriminated then they must form a linearly independent set.

(b) (more difficult) Show that if the states are linearly independent then they can be unambiguously discriminated. (It may help to begin by adjoining an n-dimensional ancilla.)