QUANTUM INFORMATION AND COMPUTATION
EXERCISE SHEET 2

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

(1) (Generalised Pauli operations for dimension d)
For a d-dimensional quantum system (a so-called qudit) with orthonormal basis $\{|j\rangle : j \in \mathbb{Z}_d\}$, introduce the operations X and Z defined by their actions on basis states:

$$X\,|j\rangle = |j+1 \bmod d\rangle \qquad Z\,|j\rangle = w^j\,|j\rangle$$

where $w = e^{2\pi i/d}$. Note that X and Z are unitary (why?) but not Hermitian (unless $d = 2$).

(a) Show $ZX = wXZ$, $X^d = Z^d = I$ and express $(X^a)^\dagger$ and $(Z^b)^\dagger$ in terms of X and Z for $a, b \in \mathbb{Z}_d$.

(b) Show that $\mathrm{Tr}\,(X^a Z^b) = 0$ for all $(a,b) \in \mathbb{Z}_d \times \mathbb{Z}_d$ except $(a,b) = (0,0)$.

(c) Consider the 2-qudit state $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle\,|i\rangle$. Show that for any operator V on one qudit, we have $\mathrm{Tr}\,V = d\,\langle\Phi|\, V \otimes I\,|\Phi\rangle$. (Here $\mathrm{Tr}\,V$ is the trace of the matrix of V with respect to the orthonormal qudit basis of $|i\rangle$'s, and this trace is in fact independent of choice of qudit orthonormal basis).

(d) Using the above, invent a quantum dense coding scheme for d dimensional systems (generalising the basic case of $d = 2$).
(Remark: the same formalism can be used to also give a quantum teleportation scheme for qudits too.)

(e) If $d = 2^n$ (i.e. the qudit is isomorphic to a composite system n qubits) how does the scheme in (d) compare to the use of the basic qubit dense coding scheme (as in lectures) applied separately on each on n qubits?

(2) (Teleporting entanglement)
(a) Alice holds an entangled state $|\alpha\rangle_{A'A}$ of two qubits $A'A$ and she teleports qubit A to Bob i.e. she just applies the standard teleportation protocol to qubit A. Show that the teleportation preserves entanglement i.e. that at the end, Bob's qubit B will be entangled with A' just as A was, so that Alice and Bob will jointly hold the state $|\alpha\rangle_{A'B}$.

(b) (entanglement swapping, aka quantum repeater)
Alice (A) and Bob (B) are separated by distance $2d$ and wish to share a $|\phi^+\rangle$ Bell state. However because of environmental effects (maybe air pollution), flying qubits (maybe photonic polarisation qubits) retain their entanglement properties only up to a distance d so A cannot just locally prepare $|\phi^+\rangle$ and send one of its qubits over to B. Their friend Charlie (C) is positioned midway between A and B (i.e. distance d away from each) and has shared a $|\phi^+\rangle$ state with each of them. Show how C can then grant A and B their wish by using only local operations at C and classical communication to other parties.
Remark: thus if we can directly set up entanglement only over a (possibly small) bounded distance, then by repeating the above process (hence "quantum repeater") we establish entanglement over arbitrarily large distances, and entangle particles that have never been near to each other (hence "entanglement swapping").

(3) (Intercept-resend attack in BB84 QKD)
A general orthonormal qubit basis can be expressed as
$\mathcal{B}(a,b) = \{\, |\beta_0\rangle = a\,|0\rangle + b\,|1\rangle \;,\; |\beta_1\rangle = -b^*\,|0\rangle + a^*\,|1\rangle \,\}$
where $a, b \in$, $|a|^2 + |b|^2 = 1$ and * denotes complex conjugation.
Alice and Bob are distantly separated in space. They can communicate classically and are also connected by a noiseless quantum channel. They perform BB84 quantum key distribution.

Suppose Eve, hiding in between, attempts to eavesdrop by following the intercept-resend strategy, measuring each passing qubit in the basis $\mathcal{B}(a, b)$ and sending on the post-measurement state to Bob. Eve interprets her measurement outcome $|\beta_i\rangle$ as bit value i.

(a) Calculate the average bit error rate, as a function of a and b, that Eve's action will cause in Alice and Bob's strings. Calculate also the probability that Eve learns Alice's encoded bit correctly.

(b) Show that the minimum bit error rate can be achieved by using *real* values of a and b i.e. if Eve is trying not to be detected then use of complex a and b does not help.

(c) Let $a = \cos\theta$ and $b = \sin\theta$ with $0 \leq \theta \leq \pi/2$. For what value of θ does Eve cause the least disturbance i.e. minimum bit error rate? For what value of θ does Eve gain the most information i.e. maximum probability of learning Alice's bit?

(4) (Positive operators, more on state distinguishability)
(a) An operator P is called *positive* if P is Hermitian and for all $|\psi\rangle$, $\langle\psi| P |\psi\rangle$ is real with $\langle\psi| P |\psi\rangle \geq 0$. (Remark: actually $\langle\psi| P |\psi\rangle$ being real for all $|\psi\rangle$ already implies that P is Hermitian, as you might like to show.)
(i) Show that any projection operator is positive.
(ii) Show that if P is positive and Π is a projection then $\Pi P \Pi$ is positive.
(iii) Show that if P is positive then $\langle\psi| P |\psi\rangle \leq \mathrm{Tr}\, P$ for any normalised $|\psi\rangle$. (It may help to consider the eigenvalues and eigenbasis of P.)

(b) Alice sends Bob one of N equally likely states $|\alpha_k\rangle$ for $k = 1, \ldots, N$, each being a state in d dimensions, representing the message k. On receiving the state Bob attempts to read Alice's message by first adjoining an ancilla $|A\rangle$ to the received state and then performing a measurement on the total state, with projectors Π_k, $k = 1, \ldots, N$ respectively for concluding that the message was k.
(i) Write down an expression for the probability P_S that Bob will correctly identify Alice's intended message k.
(ii) Show that for any measurement we have $P_S \leq d/N$.
(Hint: results from (a) may be useful here, including use of (a)(ii) with Π there being projection onto the span of the N states $|\alpha_k\rangle |A\rangle$ in the enlarged space with the ancilla. Show that this subspace has dimension at most d, so the projection has trace at most d.)

Thus we see that d-dimensional states can never be used to reliably send more than d messages, and if we attempt to use larger N's then the success probability will be correspondingly necessarily worse. Is the bound d/N on P_S here tight for a given set of N states $|\alpha_k\rangle$ in d dimensions? Give a reason for your answer.

(5) (Quantum money) (Optional question, do if time permits)
(S. Wiesner's unforgeable quantum banknotes)
A quantum banknote has printed on it a *serial number* which is an N-bit string, visible to all. It also has N *qubits* embedded in it (assumed to be perfectly stable, perhaps tastefully adorning a holographic image of the reigning monarch). For each such banknote, the bank also sets up a further N-bit string called the *basis string* and keeps this string *secret*. When the note is manufactured, the serial number on it is encoded into the N qubits using the standard BB84 encoding scheme for the serial number bits 0 and 1 (viz. 0 encoded as $|0\rangle$ or $|+\rangle$, and 1 encoded as $|1\rangle$ or $|-\rangle$ for the corresponding basis bit string bit being 0 or 1 respectively).

Now when the note is returned to the bank after financial transaction, the bank *tests the note for authenticity* as follows: the bank teller measures each of the N qubits in the basis given by the corresponding basis string bit (known only to the bank) and accepts the banknote only if *all* measurements give the correct result viz. the corresponding bit values of the serial number.

A counterfeiter wants to make fake notes that will pass this test. He/she clearly can read the serial number's bits but does not know the qubit encoding bases.

(a) Show that a genuine banknote will always pass the test and remain genuine after the test.

(b) Consider the k^{th} qubit on the note. What is the maximum probability that the counterfeiter can determine the k^{th} basis string bit by a measurement on the qubit?

(c) The counterfeiter tries to identify the k^{th} basis string bit as in (b) and then uses the result to correspondingly set the state of the k^{th} qubit on a fake banknote (printed with the same serial number string). If subsequently inspected by the bank, what is the probability that the k^{th} qubit will pass the inspection?
Now suppose the note has $N = 100$ qubits on it. What is the probability that the fake note (with each qubit set by the counterfeiter, as above) will be accepted as genuine by the bank?

(6) (Gate teleportation)
(a) Suppose we perform the standard teleportation protocol up to and including Alice's measurement, but instead of using $|\phi^+\rangle_{AB}$ we use the state $|\phi_U\rangle_{AB} = I_A \otimes U_B\, |\phi^+\rangle_{AB}$ in its place. Here U is any one-qubit unitary gate.
Show that each outcome ij of Alice's measurement will again occur with probability 1/4 but now the corresponding states of Bob's qubit will be $UP_{ij}\,|\alpha\rangle$ where $P_{ij}\,|\alpha\rangle$ are the corresponding states in standard teleportation.
Hence upon subsequently receiving the information of ij, if Bob applies the correction operators $R_{ij} = UP_{ij}^{\dagger}U^{\dagger}$ he will obtain $U\,|\alpha\rangle$ in every case.

(b) In some cases the correction operators are simple. For $U = H$ calculate the corresponding operators R_{ij}.

(c) Suppose we have a plentiful supply of $|\phi^+\rangle$ states and can easily reliably perform Bell measurements as well as Pauli gates on any qubits. We also have an H-gate machine but it functions correctly only half the time and it also signals whether it has failed or succeeded.
We have one copy of a precious qubit state $|\alpha\rangle$ and we want to make $H\,|\alpha\rangle$. Show how this may be achieved with any high success probability $1 - \epsilon$ (for any $\epsilon > 0$).

(7) (B92 quantum key distribution)
We'll describe a quantum key distribution scheme (devised by C. Bennett in 1992) that uses only *two* non-orthogonal qubit states viz. $|0\rangle$ and $|+\rangle$, instead of the four states used in BB84.

Alice first generates a uniformly random N bit string $x = x_1x_2\ldots x_N$ (a subset of which will provide the shared secret key). She encodes these bits into qubit states using $|0\rangle$ for bit value 0 and $|+\rangle$ for bit value 1. Then she sends them over to Bob (in order). For each received qubit, Bob randomly (with probability half) chooses to measure it in the Z eigenbasis or the X eigenbasis.

(a) Show that for some of Bob's possible measurement outcomes he can correctly learn Alice's corresponding bit and know for sure that he has learnt it. For what fraction μ on average, of Alice's bits, will this happen (assuming a perfectly noiseless quantum channel and no eavesdropping)?

Next in the B92 protocol, Bob (publicly) announces to Alice the positions (i.e. subscripts $1 \leq i \leq N$) for which he has learnt her bit (but does not disclose the bit values themselves!), and they both retain only these bits, discarding all the others. In the ideal situation of a noiseless channel and no eavesdropping, the resulting string (of average length μN) gives the desired shared secret key.

(b) To get an idea of the effects of attempted eavesdropping in the B92 protocol, we'll look only at a simple example of an intercept-resend attack by Eve, while assuming the qubit channel is noiseless. Suppose that Eve measures each passing qubit in the Breidbart basis and sends the post-measurement state on to Bob.
Consider only those qubits for which Alice sent $|0\rangle$. (A similar analysis will apply for $|+\rangle$). Show that the fraction μ of these for which Bob will think that he has learnt Alice's bit, is the same as the value of μ in (a). Show that for these bits, the bit error rate will be 1/2 i.e. Bob will conclude the wrong value of Alice's bit for half of these on average.

(8) (Approximate cloning) (Optional question, do if time permits)
Let $|\alpha_0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ and $|\alpha_0\rangle = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle$ be two qubit states (for a fixed chosen value of $0 < \theta < \pi/2$).
We know that these states cannot be perfectly cloned so consider an approximate cloning machine $\mathcal{M}_\theta$ of the following kind:
on input $|\alpha_0\rangle|0\rangle$ the output is a 2-qubit state $|c_{00}\rangle$; and
on input $|\alpha_1\rangle|0\rangle$ the output is a 2-qubit state $|c_{11}\rangle$.
Here $|c_{jj}\rangle$ (generally possibly entangled) is our approximate cloning result for $|\alpha_j\rangle$ i.e. our approximation for $|\alpha_j\rangle|\alpha_j\rangle$. The *cloning fidelity* for $|\alpha_j\rangle$ is defined to be $F_{\rm cl}(j) = |\langle\alpha_j|\langle\alpha_j|c_{jj}\rangle|^2$ (so cloning fidelity 1 would mean perfect cloning). The cloning machine $\mathcal{M}_\theta$ is required to have the following properties:
(P1): it is a *unitary* operation on the two qubits;
(P2): it has *equal* cloning fidelity for both $|\alpha_0\rangle$ and $|\alpha_1\rangle$;
(P3): the states $|c_{00}\rangle$ and $|c_{11}\rangle$ lie in the two dimensional span of $|\alpha_0\rangle|\alpha_0\rangle$ and $|\alpha_1\rangle|\alpha_1\rangle$ and furthermore, in the standard qubit basis, they both have *real* amplitudes.

(a) Subject to the above constraints, find the optimal achievable value of $F_{\rm cl}(j)$, and show that if $\theta = \pi/4$ then the optimal cloning fidelity is $\cos^2(\pi/24)$.

(b) A more general kind of approximate cloning machine allows intermediate measurements and probabilistic choices too, resulting in a variety of possible outputs $\left|c_{jj}^{(m)}\right\rangle$ (for each input $|\alpha_j\rangle$), occurring with known probabilities $p_{m,j}$ determined by the specification of the process. The cloning fidelity is then defined to be the $p_{m,j}$-average $F_{\rm cl}(j) = \sum_m p_{m,j}\,|\langle\alpha_j|\langle\alpha_j|c_{jj}^{(m)}\rangle|^2$. Use the theorem on optimal discrimination of two non-orthogonal states as given in lectures, to design an approximate cloning machine $\mathcal{N}_\theta$ of this more general sort.

For the case of $\theta = \pi/4$, identify explicitly the optimal qubit measurement for distinguishing these states. Then compare the cloning fidelity of $\mathcal{N}_{\pi/4}$ with that of $\mathcal{M}_{\pi/4}$ in (a), to see that cloning by first trying to classically identify the state (and then producing two copies of the result) is generally not as good as a process that bypasses attempted identification, and stays "intrinsically quantum" all the way.

[Remark: in (a) I'd expect(?) the value of $F_{\rm cl}(j)$ there to remain optimal for any unitary cloner having equal cloning fidelities for the two states (i.e. if the last condition (P3) is lifted) but I guess the argument would be more complicated.]