Quantum Computing: Example Sheets 1 and 2

1. Let $\rho = \sum_{i,j} \rho_{ij} |i\rangle\langle j|$ be the density operator of some quantum system. Show that the system is in a pure state if and only if every row of the matrix ρ_{ij} is a multiple of the first row, and every column is a multiple of the first column.

2. Show that the entropy $S(\rho) = -\mathrm{tr}_{\mathcal{H}}(\rho \ln \rho)$ obeys $S(U\rho U^\dagger) = S(\rho)$ for any unitary operator U, and hence that the entropy is both time independent and independent of the choice of basis on $\mathcal{H}$.

A composite system is formed from two uncorrelated subsystems A and B. Both subsystems are in impure states, with the numbers $\{p_i^A\}$ and $\{p_r^B\}$ being the probabilities of the members of the complete sets of states $\{|A;i\rangle\}$ and $\{|B;r\rangle\}$, respectively. Show that the entropy of the composite system is the sum of the entropies of the two subsystems. What is the relevance of this result for thermodynamics?

3. 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.

Can $|A_k\rangle$ for $k = 0$ or 1 be prepared from $|0\rangle|0\rangle$ by applying unitary operators to each individual qubit (also known as 1-qubit gates)? Give a reason for your answer.

Show that $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ is entangled iff $\alpha\delta - \beta\gamma \neq 0$.

4. Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be any 1-qubit quantum state. Suppose we receive one of the four states $|\psi\rangle, X|\psi\rangle, Y|\psi\rangle, Z|\psi\rangle$ with equal prior probabilities of 1/4. (This is known as *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 $|\psi\rangle$.)

5. 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.

Introduce the 1-qubit gate that rotates by a phase 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

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

Deduce that for any α, β, measurements on either qubit in the original basis yield 0 or 1 with equal probability. Show that this holds even if the other qubit has already been measured. (This demonstrates the no-signalling principle.)

b. Suppose both A and B measure their held qubit in the original basis. (The order of simultaneity does not matter.) Show that for the two bit outcome obtained from the two local measurements,

$$\text{prob(outcomes differ)} = \sin^2(\alpha - \beta).$$

c. We now consider only three angle settings, $\theta = -\pi/6, 0$, and $\pi/6$. Let $M_A(\alpha)$ denote the following operators for Alice: apply $U(\alpha)$ and measure in the computational basis. A similar definition holds for $M_B(\beta)$ for Bob. The experiment $E(\alpha, \beta)$ is as follows: 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 $|()\psi)$, the local operations are done essentially simultaneously. 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

(ii) $E(0, -\pi/6)$: prob(differ) = 1/4

(iii) $E(\pi/6, 0)$: prob(differ) = 1/4

(iv) $E(\pi/6, -\pi/6)$: prob(differ) = 3/4

By considering these sequences and the correlations between them implied by (i) to (iv) above, argue that it is classically 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).

6a. By inspection, 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 singular value decomposition theorem for matrices. Here we will need it just for 2×2 matrices. Write 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 a pair of qubits.

c. Let $\{|\alpha_0\rangle = a|0\rangle + b|1\rangle, |\alpha_1\rangle = c|0\rangle + d|1\rangle\}$ be an orthonormal basis for a qubit. Show there is a 1-qubit unitary U with $U|0\rangle = |\alpha_0\rangle$ and $U|1\rangle = |\alpha_1\rangle$. Hence, or otherwise, show any 2-qubit state can be prepared from $|0\rangle|0\rangle$ using 1-qubit gates and at most one CX gate. For which states is CX not required?

d. The Schmidt form does *not* generalise to tri-partite systems. To see this, show that there are states $|\psi\rangle_{ABC}$ that cannot be expressed as

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

for any bases $\{|\alpha_i\rangle\}, \{|\beta_i\rangle\}, \{|\gamma_i\rangle\}$. (Start from the Schmidt form for bipartition A vs. BC.)

7a. Let $|\xi_i\rangle, |\eta_i\rangle$ for $i = 0, 1$ be two pairs of states. Show that if $\bar{\xi_0}\xi_1\rangle = \langle\eta_0|\eta_1\rangle$, then there is a unitary U with $U|\xi_i\rangle = |\eta_i\rangle$ for $i = 0, 1$.

b. We wish to clone two distinct non-orthogonal states $|\alpha_i\rangle$, with $i = 0, 1$. We know that cloning is impossible but, in addition to $|\alpha_i\rangle$, we are also given some extra information about the states in the form of states $|\beta_i\rangle$. Show that we can only produce a second copy of $|\alpha_i\rangle$ if $|\alpha_i\rangle$ can be created from $|\beta_i\rangle$ alone. (i.e. the extra assistant state $|\beta_i\rangle$ must contain the full information about $|\alpha_i\rangle$.)

8. A *deleting operation* for the states $|\alpha_i\rangle$ acts as

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

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

Show that if such a deleting operation is unitary, then $|\alpha_i\rangle$ can be recovered from $|M_i\rangle$ alone.

Show that quantum information can be deleted if measurements are allowed.

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

9. Let $|\psi_0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|\psi_1\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$ with $0 \le \theta \le \pi/4$. Define the operator U_α by

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

Show 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 onto the two-dimensional subspace spanned by $|00\rangle$ and $|01\rangle$.

Construct a scheme for unambiguous discrimination of the states$|\psi_i\rangle$. Show the failure probability is $|\langle\psi_0|\psi_1\rangle|$.

What should we do it $\pi/4 \leq \theta \leq \pi/2$? Can the states still be unambiguously discriminated?

10. Let $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle\}$ be 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.

Show that if the states can be unambiguously discriminated, then they are linearly independent.

Show that if they are linearly independent, then they can be unambiguously discriminated. (Hint: use an n-dimensional ancilla.)

11. 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:

$$X|j\rangle = |j+1 \bmod d\rangle \quad \text{and} \quad Z|j\rangle = w^j|j\rangle, \quad \text{where } w = e^{2\pi i/d}$$

Note that X and Z are unitary (why?) but not Hermitian (unless $d = 2$).

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

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

(iii) 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

$$\mathrm{Tr}\, V = d\langle\Phi|V \otimes I|\Phi\rangle$$

(iv) Using the above, invent a quantum dense coding scheme for d-dimensional systems (generalising the basic case of $d = 2$).

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

12a. Alice holds an entangled state $|\alpha\rangle_{A'A}$ of two qubits $A'A$ and she teleports qubit A to Bob (i.e., applies the standard teleportation protocol). Show that the teleportation preserves entanglement: Bob's qubit B will be entangled with A' just as A was, so that Alice and Bob jointly hold $|\alpha\rangle_{A'B}$.

b. Alice (A) and Bob (B) are separated by distance $2d$ and wish to share a $|\phi^+\rangle$ Bell state. However, due to environmental effects, qubits retain entanglement properties only up to distance d. Their friend Charlie (C), midway between A and B, has shared a $|\phi^+\rangle$ state with each of them. Show how C can help A and B share entanglement using only local operations and classical communication.

[Remark: this is known as a *quantum repeater* and allows entanglement over large distances via *entanglement swapping*.]

13. A general orthonormal qubit basis can be expressed as

$$B(a,b) = \{|\beta_0\rangle = a|0\rangle + b|1\rangle, \quad |\beta_1\rangle = -b^*|0\rangle + a^*|1\rangle\}$$

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.

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

(i) 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.

(ii) Show that the minimum bit error rate can be achieved using *real* values of a, b.

(iii) 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?

14a. An operator P is called positive if P is Hermitian and for all $|\psi\rangle$, $\langle\psi|P|\psi\rangle$ is real and non-negative. [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 $\langle\psi|P|\psi\rangle \leq \mathrm{Tr}(P)$ for any normalized $|\psi\rangle$. (It may help to consider the eigenvalues and eigenbasis of P.)

b. Alice sends Bob one of N equally likely states $|\alpha_k\rangle$ ($k = 1, \ldots, N$), each 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, with $k = 1, \ldots, N$ respectively for concluding that the message was k.

(i) Write downthe probability P_S that Bob correctly identifies Alice's intended message was k.

(ii) Show that, for any measurement, $P_S \leq \frac{d}{N}$. (Hint: use result from Part aii), 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.)

15. 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.

(i) Show a genuine note always passes and remains genuine.

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

(iii) The counterfeiter tries to identify the k^{th} basis string bit as in (ii) 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?

16. Use modified teleportation with state $|\phi_U\rangle_{AB} = I_A \otimes U_B|\phi^+\rangle$, where U is any one-qubit unitary gate.

(i) 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.

(ii) For $U = H$, calculate R_{ij}.

(iii) 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 $\epsilon > 0$.

17. This question describes a quantum key distribution scheme known as B92 (devised by C. Bennett in 1992) that uses only two non-orthogonal qubit states $|0\rangle$ and $|+\rangle$, instead of the four states used in BB84.

Alice first generates a uniformly random N bit string $x = x_1 x_2 \ldots x_N$ (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 eaves-dropping)?

b. 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.

To get an idea of the effects of attempted eavesdropping in the B92 protocol, we will 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*

$$|\alpha_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle \quad \text{and} \quad |\alpha_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle \ .$$

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 Part a. Show that for these bits, the bit error rate will be 1/2.