Part III Quantum Information Theory: Example Sheet 1 v1.0 for example class 30th Oct, 2pm in MR14

19th October

If anything is unclear or you think you've found a mistake, please email `wm266@cam.ac.uk`. There are questions on both sides of the sheet.

1. Show that an operator $J \in \mathcal{L}(\mathcal{H})$ on a complex (and finite dimensional) Hilbert space $\mathcal{H}$ is positive (i.e. $\langle\psi|J|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$) if and only if it is hermitian and all of its eigenvalues are positive, i.e. $\lambda \geq 0$ for all $\lambda \in \mathrm{spec}(J)$. Show that, as a consequence $\langle\psi|L|\psi\rangle = \langle\psi|K|\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$ iff $L = K$. What if the Hilbert space is real?

2. Suppose that we know that, initially, a qubit Q is in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. We then learn that someone has performed a computational basis measurement on Q, but we do not learn the result of this measurement. After the measurement, what state should we assign to Q?

3. If the state of a pair of qubits AB is $\sum_{i,j=0}^{1} \alpha_{ij}|i\rangle \otimes |j\rangle$, then what is the state of A? What is the state of B? In terms of the coefficients $\alpha_{ij} \in \mathbb{C}$, when is it possible to write the state of AB as a tensor product of state vectors for the individual systems?

4. Write down a purification for the state $\frac{2}{3}|+\rangle\!\langle+|_{\mathsf{Q}} + \frac{1}{3}|-\rangle\!\langle-|_{\mathsf{Q}}$.

5. For any systems A and B such that $d_{\mathsf{A}} = d_{\mathsf{B}} = d$ we define $|\phi^+\rangle_{\mathsf{AB}} := \frac{1}{\sqrt{d}} \sum_{0\leq i<d} |i\rangle_{\mathsf{A}} \otimes |i\rangle_{\mathsf{B}}$. Recalling, from section 2.2.6 of handout one, that we take the transpose in the computational basis (i.e. $|i\rangle\!\langle j|^T = |j\rangle\!\langle i|$) prove the following

   Proposition 1 (Transpose trick)**.** Given systems A and B of the same dimension, and any $M_{\mathsf{A}} \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$, $M_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}|\phi^+\rangle_{\mathsf{AB}} = \mathbb{1}_{\mathsf{A}} \otimes M_{\mathsf{B}}^{\mathrm{T}}|\phi^+\rangle_{\mathsf{AB}}$ where $M_{\mathsf{B}} = \mathbf{id}^{\mathsf{B}\leftarrow\mathsf{A}} M_{\mathsf{A}}$.

6. In section 2.2.8 of the first handout, the Hilbert-Schmidt inner product is defined.

   (a) Show that the Hilbert-Schmidt inner product is indeed an inner product. (b) Describe a basis for the real Hilbert space $\mathrm{Herm}(\mathcal{H}_{\mathsf{Q}})$ (for arbitrary $\dim \mathcal{H}_{\mathsf{Q}} = d < \infty$) which is orthonormal in the Hilbert-Schmidt inner product on $\mathrm{Herm}(\mathcal{H}_{\mathsf{Q}})$.

7. Show that if ρ_{QR} is a density operator, then $\rho_{\mathsf{Q}} = \mathrm{Tr}_{\mathsf{R}}\rho_{\mathsf{QR}}$ is a density operator.

8. Use the composite systems postulate and the measurement postulate to derive this proposition:

   Proposition 2. Given a measurement on system A represented by a PVM E_{A}, the corresponding PVM on AB is the one which associates outcome x to $E(x)_{\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}$.

9. Give an example of a map which is positive but not completely positive.

10. Suppose that, for all $X_{\mathsf{A}} \in \mathcal{L}(\mathcal{H}_{\mathsf{A}})$: $\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}} X_{\mathsf{A}} = \sum_{j=1}^{n} K_j X_{\mathsf{A}} K_j^\dagger = \mathrm{Tr}_{\mathsf{E}} Z X_{\mathsf{A}} Z^\dagger$, where $K_j \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$ for all j and $Z \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{E}})$. Show that: $\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}$ is trace preserving $\iff \sum_{j=1}^{n} K_j^\dagger K_j = \mathbb{1}_{\mathsf{A}} \iff Z$ is an isometry.

11. Given a map $\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}$ with input dimension $d_{\mathsf{A}} = \dim(\mathcal{H}_{\mathsf{A}})$ and output dimension $d_{\mathsf{B}} = \dim(\mathcal{H}_{\mathsf{B}})$, what is the largest number of Kraus operators required to represent $\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}$? What is the largest dimension required for the system R which gets traced out in a Stinespring representation of $\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}$?

12. **Depolarising noise:** Given a qubit Q, for any $p \in [0,1]$ let $\mathcal{D}_p : \mathcal{L}(\mathcal{H}_\mathsf{Q}) \to \mathcal{L}(\mathcal{H}_\mathsf{Q})$ be the operation

$$\mathcal{D}_p : \rho \mapsto (1-p)\rho + \frac{p}{3}\left(\sigma_x \rho \sigma_x^\dagger + \sigma_y \rho \sigma_y^\dagger + \sigma_z \rho \sigma_z^\dagger\right).$$

   (a) What is the operator representation of $\mathcal{D}_p$?

   (b) Give a Stinespring representation of $\mathcal{D}_p$.

   (c) Using the Bloch ball representation of state before and after the operation,

$$\mathcal{D}_p : \ \rho[x,y,z] \mapsto \rho[x',y',z'].$$

   What is (x',y',z') as a function of (x,y,z)?

13. **Remote state preparation.**

   Alice has a qubit A and Bob has a qubit B which they prepare in the joint state $|\phi^+\rangle_{\mathsf{AB}}$ (like in the quantum strategy for the CHSH game). Taking their qubits with them (taking care to preserve their joint state), they go off to separate laboratories.

   Each person is allowed perform arbitrary measurements and time evolutions of their local system (i.e. A for Alice and B for Bob).

   Suppose Alice has some real parameter θ in mind, which is unknown to Bob.

   Describe a protocol in which the only communication between the labs is the transmission of a message taking a value in $\{0,1\}$ from Alice to Bob (via email, let's say), such that at the end of the protocol, Alice knows for sure that Bob's qubit is in the state $|\alpha_\theta\rangle := \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$.

   The transmission of the single bit is the only allowed communication or interaction between the labs.

14. **Encoding messages in states.**

   Suppose that Alice encodes a uniformly distributed (i.e. $P_X(x) = 1/k$) message X which takes one of the k values in $\mathcal{A}_X = \{1,2,\ldots,k\}$ as a state of a system Q. That is, for each possible value $x \in \mathcal{A}_X$ of the message there is some state $\rho^{(x)} \in \mathcal{H}_\mathsf{Q}$ for the system, and she prepares the system in the state $\rho^{(X)}$. To read out the message, Bob measures a POVM E with result $\hat{X}$ taking values in $\{1,2,\ldots,k\}$, which is his estimate of the message.

   Write down an expression for the success probability $\Pr(\hat{X} = X)$ and show that it cannot be larger than d_Q/k, for any choice of the states and POVM.

15. **Improving communication with entanglement.**

Suppose that, as in Question 13, Alice and Bob are again in their separate labs, with qubits A and B in the state $|\phi^+\rangle_{\mathsf{AB}}$, but this time they are linked by a noisy communication channel.

Suppose that Alice wants to send Bob a message M, with $\mathcal{A}_M = \{0, 1\}$ and $P_M(0) = P_M(1) = 1/2$, by making a *single use* of the noisy communication channel. This can't be done perfectly, but we want Bob to be make the best possible estimate $\hat{M}$ of M, in the sense that we want the probability of error

$$\Pr(\hat{M} \neq M)$$

to be as small as possible.

The input X to the channel is a pair $X = (X_1, X_2)$ where X_1 and X_2 take values in $\{0, 1\}$ and the output Y is a pair (W, V) where W takes values in $\{1, 2, \mathbf{P}\}$ and V takes values in $\{0, 1\}$. W is independent of X, and $\Pr(W = 1) = \Pr(W = 2) = \Pr(W = \mathbf{P}) = 1/3$ while V is given by

$$V = \begin{cases} X_1 & \text{if } W = 1, \\ X_2 & \text{if } W = 2, \\ (X_1 + X_2) \bmod 2 & \text{if } W = \mathbf{P}. \end{cases}$$

We can also describe the channel by writing the conditional probabilities $P_{Y|X}(y|x)$ as entries of a matrix with rows indexed by output value y and columns indexed by input value x:

$$\begin{array}{c} \\ (1,0) \\ (1,1) \\ (2,0) \\ (2,1) \\ (\mathbf{P},0) \\ (\mathbf{P},1) \end{array} \begin{array}{c} \begin{array}{cccc} (0,0) & (0,1) & (1,0) & (1,1) \end{array} \\ \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix} \end{array}$$

(a) In a classical code, Alice uses a function $e : \{0, 1\} \to \mathcal{A}_X$ to encode the message as the channel input and Bob decodes the channel output to obtain his estimate by applying a function $d : \mathcal{A}_Y \to \{0, 1\}$. That is,

$$X = e(M), \text{ and } \hat{M} = d(Y).$$

Show that the smallest probability of error that any classical code can attain is 1/6.

(b) Show that by making local measurements on their quantum systems and one use of the channel, they can achieve an error probability of $(1 - 2^{-1/2})/3 \approx 0.1$. (Hint: The PVMs they measure will be the same as they used in quantum strategy for the CHSH game, but the way they choose the measurements and use the results may be different.)