MAT3, MAMA

MATHEMATICAL TRIPOS Part III

Friday, 7 June, 2019 1:30 pm to 4:30 pm

PAPER 323

QUANTUM INFORMATION THEORY

Attempt no more than ***FOUR*** *questions.*

There are ***FIVE*** *questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS

Cover sheet
Treasury Tag
Script paper
Rough paper

SPECIAL REQUIREMENTS

None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1

(i) What does it mean to say that a bipartite state ρ_{AB} is PPT? Prove that any bipartite separable state is PPT.

(ii) Suppose σ_{AB} denotes the joint state of a qubit and a qutrit. Prove that if σ_{AB} is PPT, then it is also separable. You should carefully state any known result that you use in your proof.

(iii) Let $W := \Psi_-^{T_B} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where $\mathcal{H}_A, \mathcal{H}_B \simeq \mathbb{C}^2$, $\Psi_- = |\Psi_-\rangle\langle\Psi_-|$ with

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

and T_B denotes transposition with respect to the subsystem B.

Prove that W is an entanglement witness for the Bell state

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

[Hint: Use the fact that $\mathrm{Tr}(XY^{T_B}) = \mathrm{Tr}(X^{T_B}Y)$ for any $X, Y \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$]

(iv) A quantum channel $\Lambda : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ is said to be an *entanglement breaking (EB) channel* if $(\Lambda \otimes \mathrm{id})\rho$ is separable for all states $\rho \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$. Prove that Λ is an EB channel if and only if its Choi state is separable.

(v) A measure-and-prepare channel $\Lambda : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ is defined as

$$\Lambda(X) := \sum_a \mathrm{Tr}(E_a X)\sigma_a,$$

where $\{E_a\}_a$ is a POVM with $E_a \in \mathcal{B}(\mathbb{C}^d)$ for each a, and $\sigma_a \in \mathcal{D}(\mathbb{C}^d)$. Prove that such a channel is entanglement breaking.

(vi) Consider the quantum channel $\tilde{\Lambda} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ defined as follows: for any $X \in \mathcal{B}(\mathbb{C}^d)$,

$$\tilde{\Lambda}(X) = d \sum_j |a_j\rangle\langle a_j| \mathrm{Tr}(p_j X |b_j\rangle\langle b_j|), \tag{1}$$

where $|a_j\rangle, |b_j\rangle \in \mathbb{C}^d$, and $\{p_j\}_j$ is a probability distribution. By computing its Choi state, establish that it is entanglement breaking.

2

(i) Consider a sequence of i.i.d. random variables $X_1, X_2, \ldots, X_n$ with common probability mass function $p(x)$ with $x \in J$, where J is a finite alphabet.

(a) For a fixed $\varepsilon \in (0,1)$, when is a sequence $x^{(n)} := (x_1, x_2, \ldots, x_n)$ said to be ε-typical? Does this definition agree with the intuitive notion of a typical sequence? Justify your answer.

(b) Let $T_\varepsilon^{(n)}$ denote the set of ε-typical sequences. It is known that for any $\delta > 0$ and n large enough, the probability of the typical set, $P(T_\varepsilon^{(n)})$ is at least $(1-\delta)$. Establish an upper bound on the cardinality of the typical set in terms of the Shannon entropy $H(X) := -\sum_{x\in J} p(x) \log p(x)$.

(ii) Consider a memoryless quantum information source characterized by $\{\pi, \mathcal{H}\}$, with $\pi \in \mathcal{D}(\mathcal{H})$, with $\dim \mathcal{H} = d$. Suppose on n uses of the source, the signal $|\Psi_k^{(n)}\rangle \in \mathcal{H}^{\otimes n}$ is emitted with probability $p_k^{(n)}$, for $k \in \{1, 2, \ldots, m\}$, and let $\rho^{(n)}$ denote the density matrix associated with the ensemble $\{p_k^{(n)}, |\Psi_k^{(n)}\rangle\}$.

(a) Let the spectral decomposition of π be given by

$$\pi = \sum_{i=1}^{d} q_i |\phi_i\rangle\langle\phi_i|.$$

By considering the spectral decomposition of $\rho^{(n)}$ and evaluating its von Neumann entropy, show how one can define the ε-typical subspace $\mathcal{T}_\varepsilon^{(n)}$, for any fixed $\varepsilon \in (0,1)$. For n large enough, state an upper bound on its dimension and a lower bound on $\mathrm{Tr}(\rho^{(n)} P_\varepsilon^{(n)})$, where $P_\varepsilon^{(n)}$ denotes the projection operator onto this subspace.

(b) Schumacher's Theorem states that for $R > S(\pi)$, where $S(\pi)$ denotes the von Neumann entropy of the state π, there exists a reliable compression-decompression scheme of rate R. State precisely what is meant by reliable in this context.

(iii) Consider a memoryless classical information source characterized by a random variable X, taking values in J, where $|J| = m$. Suppose X takes the value $x_1 \in J$ with probability $(1-q)$, for some small $q \in (0,1)$. Find an upper bound on the classical data compression limit of this source.

3

(i) Suppose Alice encodes classical information in n qubits which she sends to Bob through a quantum channel. Find an upper bound on the maximum number of bits of information that Bob can infer from the output of the channel by doing measurements on it.

[Hint: Use the Holevo bound.]

(ii) Suppose Alice wants to send classical messages labelled by the elements of the set $\mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$ to Bob via multiple uses of a memoryless quantum channel $\Lambda : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$, but she can only use product state inputs. Prove that if she tries to send her messages at a rate

$$R > \max_{\{p_x, \rho_x\}} \left(S(\sum_x p_x \Lambda(\rho_x)) - \sum_x p_x S(\Lambda(\rho_x)) \right), \tag{1}$$

then the maximum probability of error does *not* vanish asymptotically, *i.e.* as $n \to \infty$, where n denotes the number of uses of Λ. Justify your steps carefully, clearly stating any assumption that you make, or any other known result that you employ in your proof.

(iii) A generalized measurement, characterized by the measurement operators $\{M_j\}_{j=1}^m$, is done on a quantum system which is initially in a pure state $\rho = |\psi\rangle\langle\psi|$. Suppose $0 \leqslant M_1 \leqslant I$, and the outcome 1 has a high probability of occurrence, *i.e.*

$$\mathrm{Tr}(M_1 \rho M_1^\dagger) \geqslant 1 - \varepsilon$$

for some small $\varepsilon \in (0, 1)$. Let ρ' denote the post-measurement state if the outcome 1 occurs. Prove that if the outcome of the measurement is 1, then the initial state ρ is not disturbed a lot, in the sense that

$$F(\rho, \rho')^2 \geqslant 1 - \varepsilon, \tag{2}$$

where $F(\rho, \rho') := ||\sqrt{\rho}\sqrt{\rho'}||_1$ denotes the fidelity between the states ρ and ρ'.

4

(i) The trace distance $D(\rho, \sigma)$ between two states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is defined as $D(\rho, \sigma) = \frac{1}{2}||\rho - \sigma||_1$. Prove that

$$D(\rho, \sigma) = \max_{0 \leqslant M \leqslant I} \operatorname{Tr}(M(\rho - \sigma)). \tag{1}$$

(ii) To any POVM $\{E_a\}_{a=1}^k$, with $E_a \in \mathcal{B}(\mathcal{H})$, where $\mathcal{H} \simeq \mathbb{C}^d$, one can associate a *measurement map* Φ defined as follows:

$$\Phi(X) = \sum_{a=1}^{k} \operatorname{Tr}(E_a X)|a\rangle\langle a|, \quad \forall\, X \in \mathcal{B}(\mathcal{H}). \tag{2}$$

Prove that Φ is a quantum operation.

(iii) Making use of the relation (1), prove that for all $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, there exists a measurement map Φ such that

$$D(\rho, \sigma) = D(\Phi(\rho), \Phi(\sigma)).$$

(iv) The so-called Pinsker's inequality states that for probability distributions $p, q \in \mathbb{R}^d$,

$$D(p||q) \geqslant \frac{1}{2\ln 2}||p - q||_1^2, \tag{3}$$

where $||p - q||_1 := \sum_{i=1}^d |p_i - q_i|$, and $D(p||q)$ denotes the classical relative entropy (or Kullback-Leibler divergence). Use this relation to prove the *quantum Pinsker inequality*: for any two states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$,

$$D(\rho||\sigma) \geqslant \frac{2}{\ln 2} D(\rho, \sigma)^2, \tag{4}$$

where $D(\rho||\sigma)$ denotes the quantum relative entropy, and $D(\rho, \sigma)$ is the trace distance.

5

(i) It is known that the quantum relative entropy is jointly convex, *i.e.*,

$$D(\sum_i p_i\rho_i || \sum_i p_i\sigma_i) \leqslant \sum_i p_i D(\rho_i||\sigma_i), \tag{1}$$

where $\{p_i\}$ denotes a probability distribution, and ρ_i, σ_i denote states.

Prove the Lindblad-Uhlmann monotonicity of the quantum relative entropy, *i.e.*, for any quantum operation Λ acting on $\mathcal{D}(\mathcal{H})$,

$$D(\Lambda(\rho)||\Lambda(\sigma)) \leqslant D(\rho||\sigma),$$

carefully stating any other properties of the quantum relative entropy that you use in your proof.

[Hint: Use (1), and the following identity:

$$\frac{1}{d^2}\sum_{k,m=0}^{d-1} W_{k,m} A W_{k,m}^\dagger = (\mathit{Tr} A)\,\frac{I}{d} \tag{2}$$

for any $A \in \mathcal{B}(\mathbb{C}^d)$, *where* $W_{k,m} := X^k Z^m \in \mathcal{B}(\mathbb{C}^d)$, *with* $k, m \in \{0, 1, 2, \ldots, d-1\}$, *are the* d^2 *unitary* Heisenberg-Weyl operators.*]*

(ii) Compute the Holevo capacity $\chi^*(\Lambda_{\text{dep}})$ of a qubit depolarizing channel Λ_{dep}, which acts on any state $\rho \in \mathcal{D}(\mathbb{C}^2)$ as follows:

$$\Lambda_{\text{dep}}(\rho) = p\rho + (1-p)\frac{I}{2}. \tag{3}$$

It is known that

$$\chi^*(\Lambda_{\text{dep}} \otimes \tilde{\Lambda}) = \chi^*(\Lambda_{\text{dep}}) + \chi^*(\tilde{\Lambda}), \tag{4}$$

for any other quantum channel $\tilde{\Lambda}$. Can the classical capacity of Λ_{dep} be increased by using entangled inputs? Justify your answer.

(iii) Prove that the quantum relative entropy satisfies the following identity:

$$\sum_j p_j D(\omega_j||\rho) = \sum_j p_j D(\omega_j||\bar{\omega}) + D(\bar{\omega}||\rho), \tag{5}$$

where $\{p_j\}$ is a probability distribution, $\rho, \omega_j \in \mathcal{D}(\mathcal{H})$, and $\bar{\omega} := \sum_j p_j \omega_j$.

(iv) Using (5), prove that

$$\min_\rho \sum_j p_j D(\omega_j||\rho) = I(X:B)_\sigma, \tag{6}$$

where

$$\sigma_{XB} = \sum_j p_j |j\rangle\langle j| \otimes \omega_j \ \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_B).$$

END OF PAPER