Problems for the MATH+ course on quantum communication and quantum networks

June 11, 2019

Problem 1 (Geometry of random compiling) *Given a completely positive map T over a Hilbert space $\mathcal{H} = \mathbb{C}^d$ for some integer d and a set of unitaries $\{U_1, \ldots, U_n\}$ on $\mathcal{H}$, (a) prove that the problem of minimizing the diamond norm*

$$\text{min} \left\| T - \sum_{j=1}^{n} p_j \mathcal{U}_j \right\|_\diamond , \tag{1}$$

$$\text{subject to} \, p_j \geq 0, \sum_{j=1}^{n} p_j = 1, \tag{2}$$

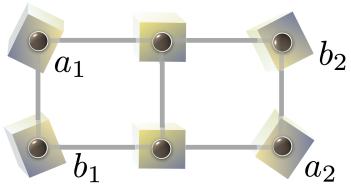
where $\mathcal{U}_j(\rho) = U_j \rho U_j^\dagger$ for all ρ, can be written as a semi-definite convex optimization problem [18]. (b) Implement this optimization problem, discuss the problem for Pauli unitaries, and (c) explain the geometry of the problem.

Problem 2 (Multi-partite quantum state manipulation in quantum networks) *Let $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ be the Hilbert space of an n-partite system. Consider pure states ρ, σ on $\mathcal{H}$. Prove (a) upper and (b) lower bounds to the rates one can achieve in asymptotic state transformations $\rho \to \sigma$ under local operations with classical communication.*

Problem 3 (Bottleneck graph states and routing problems) *Given two pairs of vertices $\{a_1, a_2\}$ and $\{b_1, b_2\}$ of a graph that is associated with a graph state vector $|G\rangle$ described by a graph $G = (V_G, E_G)$, we denote by $p_\alpha(a_1, a_2) \subset E_G$ any set of edges that describes a path connecting a_1 to a_2 and similarly $q_\beta(b_1, b_2) \subset E_G$ any set of edges that describes a path connecting b_1 to b_2 [5, 6, 11, 12]. Let G have the property that $p_\alpha \cap q_\beta \neq \emptyset$ for all α, β, i.e. every choice of paths connecting the two pairs of nodes do have at least one common edge. We would like to obtain two EPR pairs between qubits $\{a_1, a_2\}$ and $\{b_1, b_2\}$ via local Clifford operations and Z-measurements.*

(a) *Show by exhaustive search that this is not possible if* $|V_G| < 6$.

(b) *Prove that for the depicted graph state any path connecting* a_1 *to* a_2 *has at least one common edge with all paths connecting* b_1 *to* b_2.



(c) *Find a sequence of local quantum operations that create the desired EPR pairs from this graph state.*

Problem 4 (Cycle graph states) *Given a graph state vector* $|G\rangle$ *corresponding to a cycle graph, i.e. a graph* $G = (V, E)$ *with vertices* $V = \{1, \ldots, n\}$ *and edges* $E = \{(1,2), (2,3), (3,4), \ldots, (n-1, n), (n-1, n)\}$*, we want to obtain two EPR pairs between qubits* $\{a_1, a_2\}$ *and* $\{b_1, b_2\}$ *via local Clifford operations and* Z*-measurements.*

(a) *Find arrangements of* a_i, b_j *where this is not possible.*

(b) *Categorize the arrangements* a_i, b_j *where it is possible.*

Problem 5 (Quantum network games) *Ref. [7] introduces the idea of a quantum game, ref. [10] takes steps towards a mathematical theory thereof, and ref. [17] discusses quantum network games. Formulate a class of quantum network games and prove their equilibria (with Max Klimm).*

Problem 6 (Symplectic compressed sensing) *Given a bosonic continuous variable quantum system in a* pure *Gaussian state on* n *bosonic modes described by a covariance matrix* $\gamma \in \mathbb{R}^{n \times n}$ *accessible through linear measurements* $\gamma \mapsto A(\gamma)$*,*

(a) *Implement a least squares reconstruction* γ^* *of the state's covariance matrix*

$$\gamma^* = \operatorname{argmin} \|A(\gamma) - A(\gamma^*)\|_2^2 \,. \tag{3}$$

(b) *Implement a least squares reconstruction of the state's covariance matrix using the iterative hard thresholding algorithm and compare its performance to the least squares reconstruction.*

(c) Prove a recovery guarantee.

Problem 7 (Sharing classical secrets with quantum states) *Secret sharing protocols are protocols in which the secret is divided into pieces or shares by a dealer (Alice) and distributed amongst several players such that some authorized subsets can perfectly reconstruct the secret but all other subsets gain no information whatsoever. An (n,k)-threshold scheme involves n players of which any k players can collaborate to reconstruct the secret, whilst any $(k-1)$ subset remains totally ignorant. Ref. [13] introduces an elegant scheme for provably secure sharing of a classical secret using multipartite entangled states. The simplest example is the (2,2)-threshold scheme based upon the tripartite GHZ state vector $|\psi\rangle = (|0,0,0\rangle + |1,1,1\rangle)/\sqrt{2}$ distributed amongst the Alice and two potentially dishonest players, Bob and Charlie.*

(a) ***Reconstructing Alice's measurement.*** *Explicitly calculate the conditional state of Bob, for all possible measurement choices and outcomes for Alice and Charlie. Explain how Bob and Charlie can co-operate to determine Alice's measurement outcome for certain basis choices. Which choices allow for perfect reconstruction? What happens if the parties make the 'wrong' choice?*

(b) ***Security against intercept-resend attack.*** *Suppose that Bob is dishonest and that he has managed to get a hold of Charlie's particle as well as his own. He then measures the two particles and sends one of them on to Charlie. His object is to discover what Alice's bit is, without any assistance from Charlie, and to do so in a way that cannot be detected. Alice has measured her particle in either the X or Y basis, but Bob does not know which. Assuming Bob also does not know Charlies basis choice, explain how he can attempt to cheat by measuring both particles in the entangled bases. Under what conditions does Bob learn Alice's bit? Show explicitly how his attack works. If Alice randomly chooses runs of the protocol and demands Bob and Charlie announce their measurement outcomes so she can check if they are compatible with her measurement outcome, derive the minimum error probability she will find if Bob has made an intercept-resend attack.*

(c) ***Connection to stabilizers.*** *The procedure described above for Alice to check for security for the (2,2) protocol is equivalent to checking a subset of the stabilizer relations for the multipartite state. Write down the stabilizer group for the tripartite GHZ state and show this equivalence explicitly. How would the protocol have to change to check all of the stabilizer relations? What would be the downside of doing this?*

(d) ***General (non-robust) security for an*** (n,n) ***protocol.*** *In part b) you showed security against a particular attack by a dishonest party. A general security*

proof allows us to make a statement about the underlying state based only on the observed data, without making any assumptions about the action of the dishonest parties. An (n, n) secret sharing protocol begins with Alice making an $n + 1$-partite GHZ state vector, so initially we would have

$$|\psi\rangle = |GHZ(n+1)\rangle \otimes |\psi\rangle_E \tag{4}$$

where $|\psi_E\rangle$ is an auxiliary state vector of a potential eavesdropper (who might also be one of the players). Alice keeps one part of the GHZ state for herself and distributes one part to each of the n players over a potentially insecure quantum network. Any action by dishonest parties can be represented by a unitary acting on this joint state, which leads to a final state vector $|\phi\rangle = U|\psi\rangle$. Using your knowledge of stabilizer states, generalize the above protocol to (n, n)-secret sharing and show that the only way for the check to always pass (i.e. to observe an error probability of zero) is if there is no non-trivial interaction and $|\phi\rangle = |\psi\rangle$.

Problem 8 (Quantum super-dense coding) *In this protocol [2], Alice and Bob exploit some pre-shared entanglement to transmit 2 classical bits of information whilst transmitting only a single qubit.*

(a) ***Qubit example.*** *Prove that Alice can use a pre-shared Bell pair to transmit 2 classical bits by transmitting one qubit to Bob.*

(b) ***Resource relations and duality with teleportation.*** *Quantum communication resources are often classified as either static or dynamic. A static classical resource (two correlated classical bits) is written $[cc]$ whilst a static quantum resource (an entangled state) is written $[qq]$. Conversely a dynamic resource classical resource (a classical channel) is written $[c \to c]$ and a dynamic quantum resource (a quantum channel) is written $[q \to q]$. Protocols usually involve transforming one set of resources into another. What is the resource relation for superdense coding? Write down the resource relation for teleportation [1, 14] and argue why these protocols are 'dual' to one another.*

(c) ***Bosonic classical communication.*** *For a quantum channel T, the single-shot classical channel capacity (where symbols draws according to probability p_i are encoded into quantum states ρ_i) is given by the Holevo bound*

$$C_{c,1}(T) := \max_{\{p_i,\rho_i\}} \left(S(\sum_i p_i T(\rho_i)) - \sum_i p_i S(T(\rho_i)) \right). \tag{5}$$

For an identity channel ($T = \mathrm{id}$), prove that for a fixed mean photon number, $\bar{n}$, the optimal channel capacity is achieved by sending photon number states n according the probability

$$p_n = \frac{1}{1+\bar{n}} \left(\frac{\bar{n}}{1+\bar{n}} \right)^n . \tag{6}$$

(d) ***Bosonic superdense coding.*** *Explain how Alice and Bob can carry out a bosonic super-dense coding protocol using a two-mode entangled state vector*

$$|\psi\rangle = (1-\chi^2)^{1/2} \sum_{n=0}^{\infty} \chi^n |n\rangle|n\rangle \tag{7}$$

where $\chi \in [0,1]$ as outlined in ref. [3].

Problem 9 (Quantum gate teleportation) *Ref. [9] introduced the first quantum gate teleportation protocol. The latter implements the operation $|\psi\rangle \mapsto U|\psi\rangle$ among distant parties, where U is a single qubit diagonal gate. A generalized formalism for gate teleportation was described in ref. [19].*

(a) *Use the latter to derive a protocol for the teleportation of any multi-qubit diagonal gate D acting on n-qubits, for any $n \geq 1$.*

(b) *Derive a teleportation gadget by applying [19, (7)] to a multi-qubit input, similarly to examples IV.A (T-gate) and IV.B (controlled-S gate) in that work.*

Problem 10 (Delegated quantum computation) *Refs. [15, 16] introduced the model of measurement based quantum computation (MBQC), wherein a universal quantum computation is driven by adaptive single-qubit measurements acting on a multipartite resource state. Ref. [4] used this model to show how to do "delegated blind quantum computation" between a client and a server. Based on the formalism laid out in ref. [16], (a) describe and (b) prove the functioning a simple MBQC protocol where a "classical" client (Alice, who has no quantum computer) exchanges classical communication with a "quantum" server (Bob, who has a quantum computer) in order to implement a "universal" set of two-qubit gates.*

Problem 11 (Quantum parallelization) *Universal MBQC protocols require sequential adaptive operations, which can require a lot of classical communication to be exchanged in a delegated setting. Here, we will show less communication is necessary for implementing Clifford gates.*

(a) *Explain (1) how quantum circuits in the Clifford group can be realized in a single measurement step in MBQC, shown in ref. [16] using the stabilizer formalism [8].*

(b) *Prove that this requires less classical communication in a delegated setting.*

References

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70** (1993), 1895–1899.

[2] C. H. Bennett and S. J. Wiesner, *Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states*, **69** (1992), no. 20, 2881–2884.

[3] S. L. Braunstein and H. J. Kimble, *Dense coding for continuous variables*, Phys. Rev. A **61** (2000), no. 4, 042302.

[4] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal blind quantum computation*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science (2009).

[5] B. Courcelle and S.-I. Oum, *Vertex-minors, monadic second-order logic, and a conjecture by Seese*, J. Comb. Th. B **97** (2007), no. 1, 91 – 126.

[6] A. Dahlberg, J. Helsen, and S. Wehner, *How to transform graph states using single-qubit operations: computational complexity and algorithms*, (2018), arXiv:1805.05306.

[7] J. Eisert, M. Wilkens, and M. Lewenstein, *Quantum games and quantum strategies*, Phys. Rev. Lett. **83** (1999), 3077–3080.

[8] D. Gottesman, *The Heisenberg representation of quantum computers*, Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, International Press, 1999.

[9] D. Gottesman and I. L. Chuang, *Quantum teleportation is a universal computational primitive*, Nature **402** (1999), 390–393.

[10] G. Gutoski and J. Watrous, *Toward a general theory of quantum games*, Proc. STOC (2007), 565–574.

[11] F. Hahn, A. Pappa, and J. Eisert, *Quantum network routing and local complementation*, arXiv:1805.04559.

[12] M. Hein, J. Eisert, and H. J. Briegel, *Multi-particle entanglement in graph states*, Phys. Rev. A **69** (2004), 062311.

[13] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A **59** (1999), no. 3, 1829.

[14] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, *Advances in quantum teleportation*, Nature Phot. **9** (2015), 641–652.

[15] R. Raussendorf and H. J. Briegel, *A one-way quantum computer*, Phys. Rev. Lett. **86** (2001), 5188–5191.

[16] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Measurement-based quantum computation on cluster states*, Phys. Rev. A **68** (2003), 022312.

[17] G. Scarpa, *Quantum communication and quantum networking*, Int. Conf. Quant. Comm. Quant. Net. QuantumComm, 2009, pp. 74–81.

[18] J. Watrous, *Semidefinite programs for completely bounded norms*, Theory of Computing **5** (2009).

[19] X. Zhou, D. W. Leung, and I. L. Chuang, *Methodology for quantum logic gate construction*, Phys. Rev. A **62** (2000), 052316.