Solutions to assignments from

CS766/QIC820 Theory of Quantum Information (Fall 2017)

University of Waterloo, Lecturer: John Watrous

Daochen Wang

November 12, 2019

Preface

This document results from a reading group I organised on the book "The Theory of Quantum Information" (TQI) by John Watrous during Fall 2018 and Spring 2019 at the Joint Center for Quantum Information and Computer Science (QuICS) of the University of Maryland. Our reading group consisted of QuICS members Sandesh Kalantre, Eddie Schoute, and myself.

We navigated TQI by following the lecture course in the title. The assignment problems from this course, all of which also appear in TQI, are reproduced at the start of this document. Following these problems are my solutions to all of them. Any numbered reference to Lemma, Proposition, Theorem, or Example refers to TQI. If I used any external resources to solve a problem, I have referenced them at the beginning of each solution. I am very grateful to John Watrous for allowing me to post these solutions online.

Assignments

Assignment 1

Due: Thursday, October 5 at 4:00pm

1. This problem is not intended to reveal anything profound—it is just meant to give you some practice in working with vectors, operators, and such.

   (a) Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $A \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ be any nonzero operator. Prove that there exists a complex Euclidean space $\mathcal{Z}$ along with vectors $u \in \mathcal{X} \otimes \mathcal{Z}$ and $v \in \mathcal{Z} \otimes \mathcal{Y}$ such that
   $$A = \big(\mathbb{1}_{\mathcal{X}} \otimes v^*\big)\big(u \otimes \mathbb{1}_{\mathcal{Y}}\big).$$
   What is the minimum possible dimension of $\mathcal{Z}$ that is required to write a given A in this way? (Unless stated otherwise, your answers should always be supported by a proof or argument of some form—so in this case you should not only give an expression for the minimum dimension of $\mathcal{Z}$, but also a proof showing that your expression is indeed the minimum possible dimension.)

   (b) Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $\Phi \in \mathrm{CP}(\mathcal{X}, \mathcal{Y})$ be a completely positive map. Prove that there exists an operator $B \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Z}, \mathcal{Y})$, for some choice of a complex Euclidean space $\mathcal{Z}$, such that
   $$\Phi(X) = B(X \otimes \mathbb{1}_{\mathcal{Z}})B^*$$
   for all $X \in \mathrm{L}(\mathcal{X})$. Identify a condition on the operator B that is equivalent to Φ preserving trace.

2. Let Σ be an alphabet, let $\mathcal{X}$ be a complex Euclidean space, and let $\phi : \mathrm{Herm}(\mathcal{X}) \to \mathbb{R}^{\Sigma}$ be a linear function. Prove that these two statements are equivalent:

   Statement 1. It holds that $\phi(\rho) \in \mathcal{P}(\Sigma)$ for every density operator $\rho \in \mathrm{D}(\mathcal{X})$.

   Statement 2. There exists a measurement $\mu : \Sigma \to \mathrm{Pos}(\mathcal{X})$ such that
   $$(\phi(H))(a) = \langle \mu(a), H \rangle$$
   for every $H \in \mathrm{Herm}(\mathcal{X})$ and $a \in \Sigma$.

   A correct solution to this problem implies that the definition of how measurements work is simply a mathematical way of representing what measurements obviously need to be: linear functions that map quantum states to probability distributions of measurement outcomes.

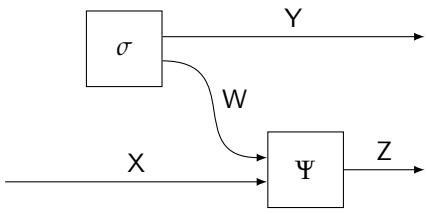
3. Interesting structural properties of channels are sometimes reflected in a simple way by their Choi representations. This problem is concerned with one example along these lines.

   Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be complex Euclidean spaces, let $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ be a channel, and consider the following two statements.

   Statement 1. There exists a density operator $\rho \in \mathrm{D}(\mathcal{Y})$ such that
   $$\mathrm{Tr}_{\mathcal{Z}}(J(\Phi)) = \rho \otimes \mathbb{1}_{\mathcal{X}}.$$

   Statement 2. There exists a complex Euclidean space $\mathcal{W}$, a density operator $\sigma \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{W})$, and a channel $\Psi \in \mathrm{C}(\mathcal{W} \otimes \mathcal{X}, \mathcal{Z})$ so that
   $$\Phi(X) = \big(\mathbb{1}_{\mathrm{L}(\mathcal{Y})} \otimes \Psi\big)(\sigma \otimes X)$$
   for all $X \in \mathrm{L}(\mathcal{X})$.

   It may be helpful to think about a channel Φ satisfying statement 2 as being one that can be implemented as the following figure suggests:



Prove that statements 1 and 2 are equivalent.

4. Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let Σ be an alphabet, and let $\eta : \Sigma \to \mathrm{Pos}(\mathcal{X})$ be an ensemble of states. Suppose further that $u \in \mathcal{X} \otimes \mathcal{Y}$ is a vector such that

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \sum_{a \in \Sigma} \eta(a).$$

Prove that there exists a measurement $\mu : \Sigma \to \mathrm{Pos}(\mathcal{Y})$ for which it holds that

$$\eta(a) = \mathrm{Tr}_{\mathcal{Y}}\big((\mathbb{1}_{\mathcal{X}} \otimes \mu(a))uu^*\big)$$

for all $a \in \Sigma$.

One interpretation of this problem is as follows. Suppose Alice holds a register X and Bob holds Y, and that the state of the pair (X, Y) is pure. If Bob performs a measurement on Y and sends the outcome to Alice, the state of X (together with Bob's measurement outcome) will be described by some ensemble η. The fact you are asked to prove implies that if Bob selects his measurement appropriately, he can cause the state of X to be described by *any ensemble he chooses*, so long as the original state purifies the average state of that ensemble.

Assignment 2

Due: Thursday, October 26 at 4:00pm

5. This first problem consists of two separate questions about the fidelity function.

   (a) This one is inspired by a question asked in the lecture (for which I did not know an answer on the spot). Give an example of two states $\rho, \sigma \in \mathrm{D}(\mathcal{X})$, for your choice of a complex Euclidean space $\mathcal{X}$, such that

   $$1 - \frac{1}{2}\|\rho - \sigma\|_1 = \mathrm{F}(\rho, \sigma) < \sqrt{1 - \frac{1}{4}\|\rho - \sigma\|_1^2}.$$

   Such an example shows that the first of the Fuchs–van de Graaf inequalities is tight, and not just in the trivial case when ρ and σ are either equal or orthogonal (where all three expressions are all equal, either to 1 or to 0, respectively).

   Hint: consider the proof of the first Fuchs–van de Graaf inequality, and think about what is needed to force the inequality to be an equality.

   (b) Let $\mathcal{X}$ be a complex Euclidean space, and define the *fidelity distance* between any two states $\rho, \sigma \in \mathrm{D}(\mathcal{X})$ as

   $$d_F(\rho, \sigma) = \min\bigl\{ \|u - v\| \,:\, u, v \in \mathcal{X} \otimes \mathcal{Y},\ \mathrm{Tr}_{\mathcal{Y}}(uu^*) = \rho,\ \mathrm{Tr}_{\mathcal{Y}}(vv^*) = \sigma \bigr\}.$$

   Here, you should assume that $\mathcal{Y}$ is a complex Euclidean space with $\dim(\mathcal{Y}) = \dim(\mathcal{X})$ (although the dimension of $\mathcal{Y}$ does not actually matter, so long as it is large enough to allow for the existence of purifications of ρ and σ). Prove that

   $$d_F(\rho, \sigma) = \sqrt{2 - 2\,\mathrm{F}(\rho, \sigma)}.$$

   Also prove that the fidelity distance obeys the triangle inequality:

   $$d_F(\rho, \sigma) \leq d_F(\rho, \xi) + d_F(\xi, \sigma)$$

   for all $\rho, \sigma, \xi \in \mathrm{D}(\mathcal{X})$.

6. This problem is concerned with an extension of Theorem 3.9 in the text. A formal statement of the problem is as follows.

   Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $H \in \mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$ be a Hermitian operator, and let $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ be a channel. Prove that these two statements are equivalent:

   Statement 1. It holds that

   $$\langle H, J(\Phi) \rangle = \max_{\Psi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})} \langle H, J(\Psi) \rangle.$$

   Statement 2. The operator $\mathrm{Tr}_{\mathcal{Y}}(HJ(\Phi))$ is Hermitian and satisfies

   $$\mathbb{1}_{\mathcal{Y}} \otimes \mathrm{Tr}_{\mathcal{Y}}(HJ(\Phi)) \geq H.$$

   The short discussion that follows is not needed to solve the problem, but is only intended to motivate it. Suppose that $\psi : \mathrm{C}(\mathcal{X}, \mathcal{Y}) \to \mathbb{R}$ is an arbitrary linear function from the set of channels $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ to the real numbers. It can be proved, for any such choice of a function ψ, that there must exist a Hermitian operator $H \in \mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$ such that $\psi(\Phi) = \langle H, J(\Phi) \rangle$ for all $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$. The aim of the problem above is therefore to prove that there is a simple criterion (represented by statement 2) that allows one to easily check, for a given channel Φ, whether or not Φ is an optimal channel for maximizing the function ψ, meaning that

   $$\psi(\Phi) = \max_{\Psi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})} \psi(\Psi),$$

   which is equivalent to statement 1.

7. Suppose $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces, $P, Q \in \mathrm{Pos}(\mathcal{X})$ are positive semidefinite operators, and $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is a trace-preserving and positive (but not necessarily completely positive) map. Prove that

$$\mathrm{F}(P, Q) \leq \mathrm{F}(\Phi(P), \Phi(Q)).$$

We already know that the inequality holds for Φ being a channel, but the proof we discussed in lecture relies on Φ being completely positive, so that proof will not work here. However, if you use the right characterization of the fidelity, the required inequality can be proved in a different way that only requires Φ to be positive and trace preserving.

8. Let X, Y, and Z be registers.

   (a) Prove that, for every state $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z})$ of these registers, it holds that

   $$\mathrm{I}(\mathsf{X}, \mathsf{Y} : \mathsf{Z}) \leq \mathrm{I}(\mathsf{Y} : \mathsf{X}, \mathsf{Z}) + 2\,\mathrm{H}(\mathsf{X}).$$

   Hint: you do not need strong subadditivity to prove this inequality.

   (b) Give an example of a state ρ for which the inequality in part (a) is an equality. In order to disqualify trivial examples, be sure that your example is such that $\mathrm{H}(\mathsf{X})$ is nonzero.

   Hint: thinking about dense coding may help you to find a simple example!

Assignment 3

Due: Thursday, November 16 at 4:00pm

9. The joint convexity of quantum relative entropy is useful for establishing fundamental and intuitive facts concerning various entropic quantities. The two problems that follow provide examples. (It is not necessary that you directly use the joint convexity of quantum relative entropy to answer the problems—you might, for instance, use a corollary of joint convexity such as strong subadditivity of von Neumann entropy.)

   (a) Prove that the Holevo information (or Holevo χ-quantity) of an ensemble cannot increase under the action of a channel.

   In more precise terms, let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ be a channel, let Σ be an alphabet, let $\eta : \Sigma \to \mathrm{Pos}(\mathcal{X})$ be an ensemble, and define an ensemble $\Phi(\eta) : \Sigma \to \mathrm{Pos}(\mathcal{Y})$ as

   $$(\Phi(\eta))(a) = \Phi(\eta(a))$$

   for each $a \in \Sigma$. Prove that $\chi(\Phi(\eta)) \leq \chi(\eta)$.

   (b) Prove that the conditional von Neumann entropy of a register X given a register Y is a concave function of the state of these registers:

   $$\mathrm{H}(\mathsf{X}|\mathsf{Y})_{\lambda\rho_0+(1-\lambda)\rho_1} \geq \lambda\,\mathrm{H}(\mathsf{X}|\mathsf{Y})_{\rho_0} + (1-\lambda)\,\mathrm{H}(\mathsf{X}|\mathsf{Y})_{\rho_1},$$

   or, equivalently,

   $$\begin{aligned}&\mathrm{H}\big(\lambda\rho_0 + (1-\lambda)\rho_1\big) - \mathrm{H}\big(\lambda\rho_0[\mathsf{Y}] + (1-\lambda)\rho_1[\mathsf{Y}]\big)\\ &\quad\geq \lambda\big(\mathrm{H}(\rho_0) - \mathrm{H}(\rho_0[\mathsf{Y}])\big) + (1-\lambda)\big(\mathrm{H}(\rho_1) - \mathrm{H}(\rho_1[\mathsf{Y}])\big),\end{aligned}$$

   for all $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ and $\lambda \in [0,1]$.

10. For every positive integer $n \geq 2$, define a unital channel $\Phi_n \in \mathrm{C}(\mathbb{C}^n)$ as

    $$\Phi_n(X) = \frac{\mathrm{Tr}(X)\mathbb{1}_n - X^{\mathsf{T}}}{n-1}$$

    for every $X \in \mathrm{L}(\mathbb{C}^n)$, where $\mathbb{1}_n$ denotes the identity operator on $\mathbb{C}^n$. Prove that Φ_n is not mixed-unitary when n is odd.

    Hint: This is proved in the book in Example 4.3 for the case that $n = 3$, but this proof will not extend to larger odd values of n. Instead, for any fixed choice of $n \geq 2$, think about an arbitrary Kraus representation

    $$\Phi_n(X) = \sum_{a\in\Sigma} A_a X A_a^*$$

    of Φ_n. Try to identify a property that *every* Kraus operator A_a must have, and then prove that no nonzero scalar multiple of a unitary operator can have this property when n is odd.

11. Let $\mathcal{X}$ be a complex Euclidean space, let $n = \dim(\mathcal{X})$, and let $\Phi \in \mathrm{C}(\mathcal{X})$ be a unital channel. Following our usual convention for singular-value decompositions, let $s_1(Y) \geq \cdots \geq s_n(Y)$ denote the singular values of a given operator $Y \in \mathrm{L}(\mathcal{X})$, ordered from largest to smallest, and taking $s_k(Y) = 0$ when $k > \mathrm{rank}(Y)$.

    Prove that, for every operator $X \in \mathrm{L}(\mathcal{X})$, it holds that

    $$s_1(X) + \cdots + s_m(X) \geq s_1(\Phi(X)) + \cdots + s_m(\Phi(X))$$

    for every $m \in \{1, \ldots, n\}$.

Hint: thinking about the block operator

$$\begin{pmatrix} 0 & X \\ X^* & 0 \end{pmatrix} = E_{0,1} \otimes X + E_{1,0} \otimes X^*$$

is helpful when solving this problem.

12. This problem asks you to prove two inequalities concerning entropic quantities that hold for separable states, but not necessarily for other states. For both inequalities, let X and Y be registers and let $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ be a separable state of these registers, expressed as

$$\rho = \sum_{a \in \Sigma} p(a) \sigma_a \otimes \xi_a,$$

for some choice of an alphabet Σ, a probability vector $p \in \mathcal{P}(\Sigma)$, and two collections of states $\{\sigma_a : a \in \Sigma\} \subseteq \mathrm{D}(\mathcal{X})$ and $\{\xi_a : a \in \Sigma\} \subseteq \mathrm{D}(\mathcal{Y})$.

   (a) Prove that, with respect to the state ρ, it holds that $\mathrm{I}(\mathsf{X} : \mathsf{Y}) \leq \mathrm{H}(p)$.
   (b) Prove that, with respect to the state ρ, it holds that

$$\mathrm{H}(\mathsf{X}|\mathsf{Y}) \geq \sum_{a \in \Sigma} p(a) \, \mathrm{H}(\sigma_a).$$

   (The conditional von Neumann entropy is therefore nonnegative for separable states.)

Assignment 4

Due: Tuesday, December 5 at 4:00pm

13. Let X and Y be registers and let $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ be a state of the pair (X, Y). With respect to ρ, one defines the *entanglement of formation* between X and Y as

$$\mathrm{E_F}(\mathsf{X} : \mathsf{Y}) = \inf \left\{ \sum_{a \in \Sigma} p(a)\, \mathrm{H}\big(\mathrm{Tr}_{\mathcal{Y}}(u_a u_a^*)\big) \;:\; \sum_{a \in \Sigma} p(a) u_a u_a^* = \rho \right\},$$

where the infimum is over all choices of an alphabet Σ, a probability vector $p \in \mathcal{P}(\Sigma)$, and a collection of unit vectors $\{u_a \,:\, a \in \Sigma\} \subset \mathcal{X} \otimes \mathcal{Y}$ for which it holds that

$$\sum_{a \in \Sigma} p(a) u_a u_a^* = \rho.$$

Now suppose that Z and W are registers and $\Phi \in \mathrm{C}(\mathcal{X} \otimes \mathcal{Y}, \mathcal{Z} \otimes \mathcal{W})$ is a channel that can be expressed as

$$\Phi(X) = \sum_{b \in \Gamma} (A_b \otimes B_b) X (A_b \otimes B_b)^*$$

for all $X \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$, for some collection of isometries $\{A_b \,:\, b \in \Gamma\} \subset \mathrm{U}(\mathcal{X}, \mathcal{Z})$ and a collection of operators $\{B_b \,:\, b \in \Gamma\} \subset \mathrm{L}(\mathcal{Y}, \mathcal{W})$ satisfying

$$\sum_{b \in \Gamma} B_b^* B_b = \mathbb{1}_{\mathcal{Y}}.$$

(Thus, $\Phi \in \mathrm{LOCC}(\mathcal{X}, \mathcal{Z} : \mathcal{Y}, \mathcal{W})$ is a one-way left LOCC channel.) Prove that

$$\mathrm{E_F}(\mathsf{Z} : \mathsf{W})_{\Phi(\rho)} \leq \mathrm{E_F}(\mathsf{X} : \mathsf{Y})_{\rho}$$

where $\mathrm{E_F}(\mathsf{X} : \mathsf{Y})_{\rho}$ and $\mathrm{E_F}(\mathsf{Z} : \mathsf{W})_{\Phi(\rho)}$ denote the entanglement of formation of the pairs (X, Y) and (Z, W) with respect to the states ρ and $\Phi(\rho)$, respectively.

Once the above inequality has been established, it is not difficult to conclude that it holds not only for channels Φ of the form described above, but for all LOCC channels Φ. You do not need to prove this as a part of your solution.

(Challenge problem.) Prove the stronger claim that the inequality

$$\mathrm{E_F}(\mathsf{Z} : \mathsf{W})_{\Phi(\rho)} \leq \mathrm{E_F}(\mathsf{X} : \mathsf{Y})_{\rho}$$

holds for all separable channels $\Phi \in \mathrm{SepC}(\mathcal{X}, \mathcal{Z} : \mathcal{Y}, \mathcal{W})$.

14. Let Σ be an alphabet, let $n = |\Sigma|$, and assume $n \geq 2$. Also let $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Sigma}$, and recall that the *swap operator* $W \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$, which satisfies $W(x \otimes y) = y \otimes x$ for all $x, y \in \mathbb{C}^{\Sigma}$, may alternatively be defined as

$$W = \sum_{a,b \in \Sigma} E_{a,b} \otimes E_{b,a}.$$

Define projections $\Pi_0, \Pi_1 \in \mathrm{Proj}(\mathcal{X} \otimes \mathcal{Y})$ and states $\sigma_0, \sigma_1 \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ as follows:

$$\Pi_0 = \frac{1}{2}\mathbb{1} \otimes \mathbb{1} + \frac{1}{2}W, \qquad \Pi_1 = \frac{1}{2}\mathbb{1} \otimes \mathbb{1} - \frac{1}{2}W, \qquad \sigma_0 = \frac{1}{\binom{n+1}{2}}\Pi_0, \qquad \sigma_1 = \frac{1}{\binom{n}{2}}\Pi_1.$$

Prove that if $\mu : \{0,1\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is a PPT measurement, meaning that μ is a measurement and $\mu(0), \mu(1) \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$, then

$$\frac{1}{2}\langle \mu(0), \sigma_0 \rangle + \frac{1}{2}\langle \mu(1), \sigma_1 \rangle \leq \frac{1}{2} + \frac{1}{n+1}.$$

(Thus, PPT measurements are not very good at discriminating between σ_0 and σ_1, even though they are orthogonal.)

15. Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be a map, for complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$. Prove that

$$|||\Phi|||_1 = \max_{\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})} \left\| \left(\mathbb{1}_{\mathcal{Y}} \otimes \sqrt{\rho_0}\right) J(\Phi) \left(\mathbb{1}_{\mathcal{Y}} \otimes \sqrt{\rho_1}\right) \right\|_1.$$

16. Let $\mathcal{X}$ be a complex Euclidean space, let $n = \dim(\mathcal{X})$, and let μ denote the uniform spherical measure on $\mathsf{S}(\mathcal{X})$.

    (a) Define a mapping $\Phi \in \mathrm{CP}(\mathcal{X})$ as

    $$\Phi(X) = n \int \langle uu^*, X \rangle \, uu^* \, \mathrm{d}\mu(u)$$

    for all $X \in \mathrm{L}(\mathcal{X})$. Give a simpler expression for Φ. Your expression should describe Φ as a convex combination of channels that we have already encountered many times in this course.

    (b) Define a channel $\Xi \in \mathrm{C}(\mathcal{X}, \mathcal{X} \otimes \mathcal{X})$ as

    $$\Xi(X) = n \int \langle uu^*, X \rangle \, uu^* \otimes uu^* \, \mathrm{d}\mu(u)$$

    for all $X \in \mathrm{L}(\mathcal{X})$. This channel might seem like it is good for cloning pure states. Calculate the value

    $$\inf_{v \in \mathsf{S}(\mathcal{X})} \langle vv^* \otimes vv^*, \Xi(vv^*) \rangle,$$

    which quantifies how good Ξ is as a pure state cloner.

    (It so happens that Ξ is a sub-optimal cloning channel, in the sense of Theorem 7.28, aside from the trivial case in which $\dim(\mathcal{X}) = 1$.)

Solutions

Assignment 1

P1a [Matrix is a vector outer product]

Proof. Let $\{e_i\}_{i=1}^n$ be an o.n. basis of $\ker(A)^\perp \subset \mathcal{Y}$ and $\{f_i\}_{i=1}^m$ be an o.n. basis of $\mathcal{X}$ where $n = \mathrm{rk}(A)$. Suppose

$$A : e_i \mapsto \sum_{j=1}^{m} a_{ji} f_j. \tag{1}$$

Then we may take $\mathcal{Z}$ to be a space with dimension $\mathrm{rk}(A)$ with an o.n. basis $\{g_i\}_{i=1}^n$. Then $A = (1_\mathcal{X} \otimes v^*)(u \otimes 1_\mathcal{Y})$ with

$$u = \sum_{i,j} a_{ji} f_j \otimes g_i \in \mathcal{X} \otimes \mathcal{Z}, \tag{2}$$

$$v = \sum_i g_i \otimes e_i \in \mathcal{Z} \otimes \mathcal{Y}. \tag{3}$$

□

Claim 1. For any choice of $\mathcal{Z}$ that satisfies the requirements, it is necessary that $\dim(\mathcal{Z}) \geq \mathrm{rk}(A)$.

Proof. Suppose $\mathcal{Z}$ has dimension N, then can let $\{z_i\}_{i=1}^N$ be an o.n. basis of $\mathcal{Z}$. Any $u \in \mathcal{X} \otimes \mathcal{Z}$ and $v \in \mathcal{Z} \otimes \mathcal{Y}$ can thus be written as

$$u = \sum_{i=1}^{N} x_i \otimes z_i, \tag{4}$$

$$v = \sum_{i=1}^{N} z_i \otimes y_i, \tag{5}$$

for some vectors $x_i \in \mathcal{X}$, $y_i \in \mathcal{Y}$. This gives

$$A = \sum_{i=1}^{N} x_i y_i^*. \tag{6}$$

Therefore the $\mathrm{rk}(A) \leq N$. □

P1b [Channels have alternative Stinespring representation]

Proof. Since Φ is completely positive, Φ^* is also completely positive by Prop. 2.18. So Φ^* has Stinespring representation

$$\Phi^*(Y) = \mathrm{Tr}_\mathcal{Z}(AYA^*), \tag{7}$$

where $A \in L(\mathcal{Y}, \mathcal{X} \otimes \mathcal{Z})$ for some $\mathcal{Z}$. Therefore $\Phi = \Phi^{**}$ has

$$\Phi(X) = B(X \otimes 1_\mathcal{Z})B^*, \tag{8}$$

where $B = A^* \in L(\mathcal{X} \otimes \mathcal{Z}, \mathcal{Y})$. □

The condition on B equivalent to Φ preserving trace is

$$\mathrm{Tr}_\mathcal{Z}(B^*B) = 1_\mathcal{X}. \tag{9}$$

P2 [Measurement is a map from observables to probability vectors]

Proof. $2 \implies 1$ is clear. For $1 \implies 2$, consider the (real) linear map

$$\Phi : \mathrm{Herm}(\mathcal{X})^{\Sigma} \to L(\mathrm{Herm}(\mathcal{X}), \mathbb{R}^{\Sigma})$$
$$\mu \mapsto \langle \mu(a), \cdot \rangle,$$

where the domain and codomain have the same (real) dimension $|\Sigma|\,(\dim \mathcal{X})^2$. But Φ has trivial kernel so it is injective and so surjective. So $\exists\, \mu$ s.t. $\Phi(\mu) = \phi$. If ϕ obeys conditions in 1, then simple arguments imply this μ defines a measurement.

□

P3 [Some channels to product space are channels from product space]

In $1 \implies 2$ below, the first sentence is a hint emailed to me by John Watrous.

Proof. $2 \implies 1$ follows straightforwardly by definition of J with $\rho = \mathrm{Tr}_{\mathcal{W}}(\sigma)$ which clearly has trace 1. That ρ is positive follows from (spectral decomposition of positive operators) + (linearity of partial trace) + (Schmidt decomposition of bipartite states).

For $1 \implies 2$, let $u \in \mathcal{Y} \otimes \mathcal{W} \otimes \mathcal{X}$ be a purification of the density matrix $\rho \otimes 1_{\mathcal{X}} \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, i.e. $\mathrm{Tr}_{\mathcal{W}}(uu^*) = \rho \otimes 1_{\mathcal{X}}$. Then $\mathrm{Tr}_{\mathcal{W}\otimes\mathcal{X}}(uu^*) = \rho = \mathrm{Tr}_{\mathcal{Z}\otimes\mathcal{X}}(J(\Phi))$. Noting that $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{X})$, Prop. 2.29 gives $\exists\, \Omega \in C(\mathcal{W} \otimes \mathcal{X}, \mathcal{Z} \otimes \mathcal{X})$ such that

$$(1_{\mathcal{Y}} \otimes \Omega)\,(uu^*) = J(\Phi). \tag{10}$$

This then gives an expression for $\Phi(X)$ in the desired form with $\Psi = \mathrm{Tr}_{\mathcal{X}} \circ \Omega$ and $\sigma = \mathrm{Tr}_{\mathcal{X}}(uu^*)$. □

P4 [Can create any ensemble using its purified average state]

Proof. Write $u = \mathrm{vec}(A)$. Then the result is equivalent to: $\mu(a)$ can be chosen such that $A\,\mu(a)^t\,A^* = \eta(a)$ for all a. Now, $\mathrm{im}(\eta) \subset \mathrm{im}(AA^*) = \mathrm{im}(A)$, where the former inclusion follows as $AA^* = \sum_{a\in\Sigma} \eta(a)$ and each $\eta(a)$ is positive. Hence the result follows directly from Lemma 2.30. □

Assignment 2

P5a [Two-way trace distance bounds on fidelity can be tight only one-way]

Consider the example $\rho = \mathrm{diag}([1/3,\ 1/3,\ 1/3,\ 0])$ and $\sigma = \mathrm{diag}([0,\ 1/3,\ 1/3,\ 1/3])$.

P5b [Fidelity distance, like fidelity but with angle replaced by distance, defines a metric]

To prove the first part, use Theorem 3.22 (Uhlmann) and the following Claim.

Claim 2. $\max_{u,v} \mathrm{Re}\langle u, v\rangle = \max_{u,v} |\langle u, v\rangle|$.

Proof. LHS $\leq$ RHS is clear, suppose the max of RHS is attained at $\hat{u}, \hat{v}$, then multiplying $\hat{u}$ by $e^{i\theta}$ does not change that max, therefore we may wlog assume $\langle \hat{u}, \hat{v}\rangle$ is real, hence RHS $\leq$ LHS. □

To prove the second part, note that the min in fidelity distance can be taken over v only and any purification u of ρ. This gives us enough freedom to simply apply the triangle inequality to prove the result.

P6 [A test that passes iff channel maximises linear functional]

The proof is essentially the same as that of Theorem 3.9 (Holevo-Yuen-Kennedy-Lax). Details as follows.

Proof. Let $\alpha = \mathrm{Tr}_{\mathcal{Y}}(\cdot) \in T(\mathcal{Y} \otimes \mathcal{X}, \mathcal{X})$, $H \in \mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$ as in the question, and $1_{\mathcal{X}} \in L(\mathcal{X})$.

Consider the SDP $(\alpha, H, 1_{\mathcal{X}})$ which has primal

$$\begin{aligned} \max_{A \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X})} \quad & \langle H, A\rangle \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathcal{Y}}(A) = 1_{\mathcal{X}}, \end{aligned} \tag{11}$$

and dual

$$\begin{aligned} \min_{B \in \mathrm{Herm}(\mathcal{X})} \quad & \langle 1_{\mathcal{X}}, B\rangle \\ \text{s.t.} \quad & 1_{\mathcal{Y}} \otimes B \geq H. \end{aligned} \tag{12}$$

It is clear that the primal and dual are both strictly feasible. Hence strong duality and complementary slackness hold.

1 $\implies$ 2: By complementary slackness, there exists feasible B such that $(1_{\mathcal{Y}} \otimes B)J(\Phi) = HJ(\Phi)$. Applying $\mathrm{Tr}_{\mathcal{Y}}(\cdot)$ gives $B = \mathrm{Tr}_{\mathcal{Y}}(HJ(\Phi))$.

2 $\implies$ 1: Note $J(\Phi)$ is clearly primal feasible and $\mathrm{Tr}_{\mathcal{Y}}(HJ(\Phi))$ is given to be dual feasible. These give primal and dual objective values that equal. So the result follows by weak duality. □

P7 [PTP maps, like CPTP maps (i.e. channels), increase fidelity]

This follows from the Stinespring representation of operator maps and the increasing of fidelity under partial trace. Details as follows. [**Warning**: the proof below is actually **incomplete** as I cannot justify why APB^* and AQB^* are positive (or can be made positive).]

Proof. Any $\Phi \in T(\mathcal{X}, \mathcal{Y})$ can be expressed as

$$\Phi(\cdot) = \mathrm{Tr}_{\mathcal{Z}}(A(\cdot)B^*), \tag{13}$$

where $A, B \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$.

Then

$$F(APB^*, AQB^*) \leq F(\Phi(P), \Phi(Q)). \tag{14}$$

But $F(APB^*, AQB^*) = F(P, Q)$ as $B^*A = 1_{\mathcal{X}}$ since Φ is trace preserving. □

Remark. 1. Note that $APB^* = K^2$ where $K = A\sqrt{P}B^*$. So APB^* is positive if K is Hermitian. However, I was unable to prove the latter.

2. Of course, the proof is complete if Φ is a channel, so $B = A$.

3. The increasing of fidelity under partial trace follows morally and immediately from Theorem 3.22 (Uhlmann).

P8 [Mutual information difference of two "overlapping" partitions can be bounded by twice entropy in overlap]

(a) Follows from Theorem 5.25.

(b) Consider $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,|0\rangle$, with registers labelled in order $(\mathcal{X}, \mathcal{Z}, \mathcal{Y})$.

Assignment 3

P9a [Holevo information of ensemble can only decrease upon application of channel]

Proof. Have

$$\chi(\eta) = D(\xi_{AX} \parallel \xi_A \otimes \xi_X), \tag{15}$$

where $\xi_{AX} = \sum_a E_{a,a} \otimes \eta_a$, $\eta_A = \sum_a p_a E_{a,a}$ with $p_a = \operatorname{Tr} \eta_a$, $\eta_X = \sum_a \eta_a$. But

$$\chi(\Phi(\eta)) = D((\mathbb{1} \otimes \Phi)\xi_{AX} \parallel (\mathbb{1} \otimes \Phi)(\xi_A \otimes \xi_X)). \tag{16}$$

So the result follows from Theorem 5.35. □

P9b [Concavity of conditional entropy]

Use the standard expression $H(X \mid Y) = -D(\rho_{XY} \parallel \mathbb{1}_X \otimes \rho_Y)$.

P10 [Proving a channel is not mixed unitary]

Proof. The Choi representation of the second equation of the question is the following equation in $L(\mathbb{C}^n \otimes \mathbb{C}^n)$ (cf. Example 4.3)

$$\sum_a \operatorname{vec}(A_a)\operatorname{vec}(A_a)^* = \frac{1}{n-1}(\mathbb{1} \otimes \mathbb{1} - W), \tag{17}$$

where W is the swap operator. Noting that the LHS is a sum of positive operators gives

$$\operatorname{vec}(A_a) \in \operatorname{im}(\mathbb{1} \otimes \mathbb{1} - W), \tag{18}$$

for all a. Now choose any A_a to write as A. Clearly $W\operatorname{vec}(A) = -\operatorname{vec}(A)$. So writing $A = \sum_{j=1}^n a_j e_j^*$, with a_j being the j-th column vector of A and e_j the standard basis vector, we deduce

$$\sum_{j=1}^n e_j \otimes a_j = -\sum_{j=1}^n a_j \otimes e_j. \tag{19}$$

We shall reach contradiction by Eq. 19, so assume A is unitary wlog. Applying $a_k^* \otimes a_l^*$ to Eq. 19 gives $A = -A^t$. Taking determinants gives the desired contradiction when n is odd. □

P11 [Unital channels can only decrease majorisation power of singular values]

The operator in given Hint is Hermitian, so Theorem 4.32 applies to give

$$\lambda\left(\begin{bmatrix} 0 & \Phi(X) \\ \Phi(X)^* & 0 \end{bmatrix}\right) \prec \lambda\left(\begin{bmatrix} 0 & X \\ X^* & 0 \end{bmatrix}\right). \tag{20}$$

The result then follows from the following three observations

$$\begin{bmatrix} 0 & X \\ X^* & 0 \end{bmatrix} v = \mu v \implies \begin{bmatrix} XX^* & 0 \\ 0 & X^*X \end{bmatrix} v = \mu^2 v, \tag{21}$$

$$\begin{bmatrix} 0 & X \\ X^* & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \mu \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \iff \begin{bmatrix} 0 & X \\ X^* & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ -v_2 \end{bmatrix} = -\mu \begin{bmatrix} v_1 \\ -v_2 \end{bmatrix}, \tag{22}$$

$$s_k(X) = \sqrt{\lambda_k(XX^*)} = \sqrt{\lambda_k(X^*X)}. \tag{23}$$

P12a [Mutual information of separable states is no greater than classical entropy of ensemble]

I used Ref. [3] in my solution (see following Remark).

Proof.

$$\begin{aligned} I(X:Y) &= D(\rho_{XY} \parallel \rho_X \otimes \rho_Y), \\ &= D(\sum_a p_a \sigma_a \otimes \xi_a \parallel \sum_a p_a (\sigma_a \otimes \sum_j p_j \xi_j)), \\ &\leq \sum_a p_a D(\sigma_a \otimes \xi_a \parallel \sigma_a \otimes \sum_j p_j \xi_j), \\ &= \sum_a p_a D(\xi_a \parallel \sum_j p_j \xi_j), \\ &= \sum_a -p_a \log p_a + D(p_a \xi_a \parallel \sum_j p_j \xi_j), \\ &= H(p) + \sum_a D(p_a \xi_a \parallel \xi), \end{aligned}$$

where $\xi := \sum_j p_j \xi_j \geq p_a \xi_a$. Therefore $D(p_a \xi_a \parallel \xi) \leq D(p_a \xi_a \parallel p_a \xi_a) = 0$. □

Remark. The last step uses Ref. [3, Prop. 11.8.2], reproduced as below Claim.

Claim 3. For $\rho, \sigma, \sigma' \in \mathrm{Pos}(X)$, have

$$\sigma' \geq \sigma \implies D(\rho \parallel \sigma') \leq D(\rho \parallel \sigma). \tag{24}$$

Proof. Since $\sigma' - \sigma \geq 0$, we have

$$\begin{aligned} D(\rho \parallel \sigma) &= D(|0 \times 0| \otimes \rho \parallel |0 \times 0| \otimes \sigma + |1 \times 1| \otimes (\sigma' - \sigma)), \\ &\geq D(\rho \parallel \sigma + \sigma' - \sigma). \end{aligned}$$

□

P12b [Conditional entropy of separable states is non-negative]

Use the standard expression $H(X \mid Y) = D(\rho_{XY} \parallel \mathbb{1}_X \otimes \rho_Y)$.

Assignment 4

P13 ["Entanglement of formation" is an entanglement monotone]

To find the following proof, I consulted the original paper defining "entanglement of formation", Ref. [1, Sec. 2.1] as well as Ref. [2, Secs. 4.3, 5.1].

Proof. Suppose we are given a decomposition

$$\rho = \sum_{a\in\Sigma} p_a \; u_a u_a^*, \tag{25}$$

then

$$\Phi(\rho) = \sum_{a\in\Sigma, b\in\Gamma} p_a \; q_{a,b} \; v_{a,b} v_{a,b}^*, \tag{26}$$

where

$$\tilde{v}_{a,b} \coloneqq (A_b \otimes B_b) u_a, \tag{27}$$
$$q_{a,b} \coloneqq \|\tilde{v}_{a,b}\|^2, \tag{28}$$
$$v_{a,b} \coloneqq \tilde{v}_{a,b} / \sqrt{q_{a,b}}. \tag{29}$$

Now, for each $a \in \Sigma, b \in \Gamma$, we have

$$\begin{aligned} H(\mathrm{Tr}_{\mathcal{W}}(v_{a,b} v_{a,b}^*)) &= H\Big(\frac{1}{q_{a,b}} \mathrm{Tr}_{\mathcal{W}}((A_b \otimes B_b) u_a u_a^* (A_b \otimes B_b)^*)\Big), \\ &= H\Big(A_b \Big[\frac{1}{q_{a,b}} \mathrm{Tr}_{\mathcal{W}}\big((1_{\mathcal{X}} \otimes B_b) u_a u_a^* (1_{\mathcal{X}} \otimes B_b)^*\big)\Big] A_b^*\Big), \\ &= H\Big(\frac{1}{q_{a,b}} \mathrm{Tr}_{\mathcal{W}}\big((1_{\mathcal{X}} \otimes B_b) u_a u_a^* (1_{\mathcal{X}} \otimes B_b)^*\big)\Big). \end{aligned} \tag{30}$$

Note that $\sum_b q_{a,b} = 1$ due to the conditions given in the question (i.e. Φ is one-way left LOCC). Then

$$\sum_{a,b} p_a \; q_{a,b} \; H(\mathrm{Tr}_{\mathcal{W}}(v_{a,b} v_{a,b}^*)), \tag{31}$$
$$= \sum_a p_a \; \sum_b q_{a,b} \; H(\mathrm{Tr}_{\mathcal{W}}(v_{a,b} v_{a,b}^*)), \tag{32}$$
$$\leq \sum_a p_a \; H\Big(\sum_b \mathrm{Tr}_{\mathcal{W}}\big((1_{\mathcal{X}} \otimes B_b) u_a u_a^* (1_{\mathcal{X}} \otimes B_b)^*\big)\Big), \tag{33}$$
$$= \sum_a p_a H(\mathrm{Tr}_{\mathcal{Y}}(u_a u_a^*)). \tag{34}$$

□

Remark. To prove the result for one-way right LOCC, note that, in the definition of E_F, the trace over $\mathcal{Y}$ (resp. $\mathcal{W}$) can be replaced by the trace over $\mathcal{X}$ (resp. $\mathcal{Z}$).

P14 [PPT measurements are useless at distinguishing between Werner states of large dimension]

Proof. Write A, B for $\mu(0)$ and $\mu(1)$ respectively and I for $\mathbb{1} \otimes \mathbb{1}$ for convenience. Now double the LHS of the original inequality is

$$\langle A, \sigma_0 \rangle + \langle B, \sigma_1 \rangle = \frac{1}{n(n+1)} \langle I + W, A \rangle + \frac{1}{n(n-1)} \langle I - W, B \rangle, \tag{35}$$
$$= 1 + \frac{2}{n(n^2-1)} \Big(\mathrm{Tr}\, B - n \,\mathrm{Tr}(WB) \Big), \tag{36}$$

where we wrote $A = I - B$ and rearranged to go from Eq. 35 to Eq. 36. Then proving the original inequality is equivalent to proving that

$$\operatorname{Tr}(B) - n \operatorname{Tr}(WB) \leq n(n-1) \tag{37}$$

$$\iff \operatorname{Tr}(B) + \operatorname{Tr}(WA) + (n-1)\operatorname{Tr}(WA) - n^2 \leq n(n-1). \tag{38}$$

Now, $\operatorname{Tr}(WA) \leq \operatorname{Tr}(A)$ by Holder's inequality. Therefore the LHS of Eq. 38 is less than or equal to $(n-1)\operatorname{Tr}(WA)$. But B being PPT gives

$$\operatorname{Tr}(WA) = n - \operatorname{Tr}(WB) \leq n. \tag{39}$$

□

Remark. The proof of $\operatorname{Tr}(WB) \geq 0$, which is the only place where the PPT condition is used, is analogous to that of Prop. 6.42.

P15 [Completely bounded trace norm in terms of Choi operator]

Proof. For convenience, write $N(\cdot)$ for the completely bounded trace norm and $\tilde{N}(\cdot)$ for

$$\tilde{N}(\Phi) := \max_{\rho,\sigma \in D(\mathcal{X})} \| (1_{\mathcal{Y}} \otimes \sqrt{\rho})\, J(\Phi)\, (1_{\mathcal{Y}} \otimes \sqrt{\sigma}) \|_1. \tag{40}$$

Prop. 3.44 says

$$N(\Phi) = \max_{u,v \in \mathcal{S}(\mathcal{X}\otimes\mathcal{X})} \| \Phi \otimes 1_{L(\mathcal{X})}(uv^*) \|_1. \tag{41}$$

But

$$\begin{aligned} &\| (1_{\mathcal{Y}} \otimes \sqrt{\rho})\, J(\Phi)\, (1_{\mathcal{Y}} \otimes \sqrt{\sigma}) \|_1 \\ &= \| (1_{\mathcal{Y}} \otimes \sqrt{\rho})\, (\Phi \otimes 1_{L(\mathcal{X})})(\operatorname{vec}(1_{\mathcal{X}})\operatorname{vec}(1_{\mathcal{X}})^*)\, (1_{\mathcal{Y}} \otimes \sqrt{\sigma}) \|_1, \\ &= \| \Big(\Phi \otimes 1_{L(\mathcal{X})} \Big) \Big([(1_{\mathcal{X}} \otimes \sqrt{\rho})\operatorname{vec}(1_{\mathcal{X}})][(1_{\mathcal{X}} \otimes \sqrt{\sigma})\operatorname{vec}(1_{\mathcal{X}})]^* \Big) \|_1, \end{aligned} \tag{42}$$

and $(1_{\mathcal{X}} \otimes \sqrt{\mu})\operatorname{vec}(1_{\mathcal{X}}) \in S(\mathcal{X} \otimes \mathcal{X})$ is the canonical purification of any $\mu \in D(\mathcal{X})$. Then

1. $N(\Phi) \geq \tilde{N}(\Phi)$ follows directly from Eq. 42.
2. $N(\Phi) \leq \tilde{N}(\Phi)$ follows from Eq. 42 together with the unitary equivalence of purifications and the unitary invariance of the trace norm.

□

P16a [Simplifying expression for channel defined by an integral]

Claim 4. Let $\Phi \in \mathrm{CP}(\mathcal{X})$ be as in the question. Writing Ω for the completely depolarising channel on $\mathcal{X}$, we find:

$$\Phi = \frac{n}{n+1}\Omega + \frac{1}{n+1} 1_{L(\mathcal{X})}. \tag{43}$$

Proof. The Choi representation of Φ is

$$J(\Phi) = n \int (u \otimes \bar{u}) \cdot (u^* \otimes \bar{u}^*)\ \mathrm{d}\,\mu(u), \tag{44}$$

$$= (1_{L(\mathcal{X})} \otimes T)\Big(n \int (uu^*)^{\otimes 2}\ \mathrm{d}\,\mu(u) \Big). \tag{45}$$

Then, Lemma 7.24 followed by Prop. 7.1 gives the Claim. □

P16b [A naive cloning channel that isn't optimal]

Claim 5. Writing N_k for the dimension $\mathrm{Sym}^k(\mathcal{X})$, the minimum cloning fidelity α of Ξ is

$$\alpha(\Xi) = \frac{N_1}{N_3}. \tag{46}$$

Proof. Take $v \in S(\mathcal{X})$, then

$$\langle vv^* \otimes vv^*, \Xi(vv^*)\rangle = n \int |\langle u, v\rangle|^6 \ \mathrm{d}\,\mu(u), \tag{47}$$

$$= N_1 \ (v^{\otimes 3})^* \ \left(\int (uu^*)^{\otimes 3} \ \mathrm{d}\,\mu(u) \right) v^{\otimes 3}, \tag{48}$$

$$= \frac{N_1}{N_3}. \tag{49}$$

□

References

[1] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A **54** (1996), 3824–3851.

[2] Michal Horodecki, *Entanglement measures*, Quantum Info. Comput. **1** (2001), no. 1, 3–26.

[3] Mark M. Wilde, *From Classical to Quantum Shannon Theory*, arXiv e-prints (2011), arXiv:1106.1445.