Some Open Problems in Quantum Information Theory

Mary Beth Ruskai*

Department of Mathematics, Tufts University, Medford, MA 02155

Marybeth.Ruskai@tufts.edu

June 14, 2007

Abstract

Some open questions in quantum information theory (QIT) are described. Most of them were presented in Banff during the BIRS workshop on Operator Structures in QIT 11-16 February 2007.

1 Extreme points of CPT maps

In QIT, a channel is represented by a completely-positive trace-preserving (CPT) map $\Phi : M_{d_1} \mapsto M_{d_2}$, which is often written in the Choi-Kraus form

$$\Phi(\rho) = \sum_k A_k \rho A_k^\dagger \qquad \text{with} \qquad \sum_k A_k^\dagger A_k = I_{d_1}. \tag{1}$$

The state representative or Choi matrix of Φ is

$$\Phi(|\beta\rangle\langle\beta|) = \tfrac{1}{d} \sum_{jk} |e_j\rangle\langle e_k| \Phi(|e_j\rangle\langle e_k|) \tag{2}$$

where $|\beta\rangle$ is a maximally entangled Bell state. Choi [3] showed that the A_k can be obtained from the eigenvectors of $\Phi(|\beta\rangle\langle\beta|)$ with non-zero eigenvalues. The operators A_k in (1) are known to be defined only up to a partial isometry and are often called Kraus operators. When a minimal set is obtained from Choi's prescription using eigenvectors of (2), they are defined up to mixing of those from degenerate eigenvalues

*Partially supported by the National Science Foundation under Grant DMS-0604900

and we will refer to them as Choi-Kraus operators. Choi showed that Φ is an extreme point of the set of CPT maps $\Phi : M_{d_1} \mapsto M_{d_2}$ if and only if the set $\{A_j^\dagger A_k\}$ is linearly independent in M_{d_1}. This implies that the Choi matrix of an extreme CPT map has rank at most d_1. We will refer to the rank of (2) as the *Choi rank* of Φ. (Note that this is *not* the same as the rank of Φ as a linear operator from M_{d_1} to M_{d_2}.)

It is often useful to consider the set of all CPT maps with Choi rank $\leq d_1$. In [24] these were called "generalized extreme points" and shown to be equivalent to the closure of the set of extreme points for qubit maps. This is true in general. Let $\mathcal{E}(d_1, d_2)$ denote the extreme points of the convex set of CPT maps from M_{d_1} to M_{d_2}.

Theorem 1. *The closure $\overline{\mathcal{E}(d_1, d_2)}$ of the set of extreme points of CPT maps $\Phi : M_{d_1} \mapsto M_{d_2}$ is precisely the set of such maps with Choi rank at most d_1.*

Proof: Let Let A_k be the Choi-Kraus operators for a map $\Phi : M_{d_1} \mapsto M_{d_2}$ with Choi rank $r \leq d_1$ which is not extreme, and let B_k be the Choi-Kraus operators for a true extreme point with Choi-rank d_1. When $r < d_1$ extend A_k by letting $A_m = 0$ for $m = r+1, r+2, \ldots d_1$ and define $C_k(\epsilon) = A_k + \epsilon B_k$. There is a number ϵ_* such that the d_1^2 matrices $C_j^\dagger(\epsilon) C_k(\epsilon)$ are linear independent for $0 < \epsilon < \epsilon_*$. To see this, for each $C_j^\dagger(\epsilon) C_k(\epsilon)$ "stack" the columns to give a vector of length d_1^2 and let $M(\epsilon)$ denote the $d_1^2 \times d_1^2$ matrix formed with these vectors as columns. Then $\det M(\epsilon)$ is a polynomial of degree d_1^4, which has at most d_1^4 distinct roots. Since the matrcies $A_j^\dagger A_k$ were assumed to be linearly dependent, one of these roots is 0; it suffices to take ϵ_* the next largest root (or $+1$ if no roots are positive). Thus, the operators $C_j^\dagger(\epsilon) C_k(\epsilon)$ are linearly independent for $\epsilon \in (0, \epsilon_*)$. The map $\rho \mapsto \sum_k C_k(\epsilon) \rho C_k^\dagger(\epsilon)$ is CP, with

$$\sum_k C_k^\dagger(\epsilon)\, C_k = (1 + \epsilon^2) I + \epsilon (A_k^\dagger B_k + B_k^\dagger A_k) \equiv S(\epsilon).$$

For sufficiently small ϵ the operator $S(\epsilon)$ is positive semi-definite and invertible, and the map $\Phi_\epsilon(\rho) = C_k(\epsilon) S(\epsilon)^{-1/2} \rho S(\epsilon)^{-1/2} C_k^\dagger(\epsilon)$ is a CPT map with Kraus operators $C_k(\epsilon) S(\epsilon)^{-1/2}$. Thus, one can find ϵ_c such that $\epsilon \in (0, \epsilon_c)$ implies that $\Phi_\epsilon \in \mathcal{E}(d_1, d_2)$. It then follows from $\lim_{\epsilon \to 0+} \Phi_\epsilon = \Phi$ that $\Phi \in \overline{\mathcal{E}(d_1, d_2)}$. **QED**

When $d_1 = 2$, one can use the singular value decomposition (SVD) to show that that the Kraus operators of CPT maps with Choi rank at most two can be written in the form

$$A_1 = \sum_{j=1,2} \alpha_j |v_j\rangle\langle u_j| \qquad A_2 = \sum_{j=1,2} \sqrt{1 - \alpha_j^2} |w_j\rangle\langle u_j| \tag{3}$$

where $0 \leq \alpha_j \leq 1$, $|u_j\rangle$ is pair of orthonormal vectors in $\mathbf{C}_2$, and $|v_j\rangle, |w_j\rangle$ are two pairs of orthonormal vectors in $\mathbf{C}_{d_2}$. This gives all CPT maps in $\overline{\mathcal{E}(2, d_2)}$. Although it may seem artificial from a physical point of view to consider $d_1 \neq d_2$, several reduction results in quantum Shannon theory require consideration of maps with $d_1 \neq d_2$.

Problem 1. *Characterize, classify and/or parameterize the closure* $\overline{\mathcal{E}(d_1, d_2)}$ *of the set of extreme points of CPT maps* $\Phi : M_{d_1} \mapsto M_{d_2}$ *for* $d_1 > 2$ *and* d_2 *arbitrary.*

Although this problem is of some interest in its own right, we will give additional motivation in Section 5.4 where we observe that certain conjectures for CPT maps with $d_1 = d_2$ can be reduced to case of the channels in the closure of extreme points with $d_1 \geq d_2$.

2 Convex decompositions of CPT maps or A block matrix generalization of Horn's lemma (with K. Audenaert)

Since the set of CPT map $\Phi : M_{d_1} \mapsto M_{d_2}$ is convex, it can be written as a convex combination of extreme maps, and one expects that $d_1^2(d_2^2 - 1)$ will suffice. For maps on qubits, it was shown in [24] that if all maps in $\overline{\mathcal{E}(d_1, d_2)}$ are permitted, then only two are needed and they can be chosen so that the weights are even. This result generalizes to any CPT map with qubit output, i.e., for $\Phi : M_d \mapsto M_2$ one can always write

$$\Phi = \tfrac{1}{2}(\Phi_1 + \Phi_2) \tag{4}$$

where Φ_1 and Φ_2 have Choi rank $\leq d$. We conjecture that this result extends to arbitrary CPT maps.

Conjecture 2. (Audenaert-Ruskai) *Let* $\Phi : M_{d_1} \mapsto M_{d_2}$ *be a CPT map. One can find* d_2 *CPT maps* Φ_m *with Choi rank at most* d_2 *such that*

$$\Phi = \sum_{m=1}^{d_2} \tfrac{1}{d_2} \Phi_m. \tag{5}$$

The adjoint or dual of a CPT map is a unital CP map and it is useful to restate the conjecture in this form.

Conjecture 3. *Let* $\Phi : M_{d_2} \mapsto M_{d_1}$ *be a CP map with* $\Phi(I_2) = I_1$*. One can find* d_2 *unital CP maps* Φ_m *with Choi rank at most* d_1 *such that*

$$\Phi = \sum_{m=1}^{d_2} \tfrac{1}{d_2} \Phi_m. \tag{6}$$

In this form, the conjecture can be viewed as a statement about block matrices, and it is useful to restate it explicitly in that form.

Conjecture 4. *Let $\mathbf{A}$ be a $d_1 d_2$ positive semi-definite matrix consisting of $d_2 \times d_2$ blocks A_{jk} each of size $d_1 \times d_1$, with $\sum_j A_{jj} = M$. Then one can find d_2 block matrices $\mathbf{B}_m$, each of rank at most d_1, such that $\sum_j B_{jj} = M$, and*

$$\mathbf{A} = \sum_{m=1}^{d_2} \tfrac{1}{d_2}\, \mathbf{B}_m \tag{7}$$

If Conjecture 4 holds, then Conjecture 3 (and hence Conjecture 2) follows immediately. One need only let $\mathbf{A} = \Phi(|\beta\rangle\langle\beta|)$ be the Choi matrix of Φ for which $M = \frac{1}{d_2} I_{d_2}$. It would suffice to prove Conjecture 5 for the case $M = I_{d_2}$. The general case then follows by multiplying on the right and left by the matrix $\frac{1}{\sqrt{d_2}}\sqrt{M} \otimes I_{d_2}$. (May be some subtleties if M is non-singular.)

When $d_1 = 1$, Conjecture 4 is a consequence of Horn's Lemma[1] [12, 13] which states that a necessary and sufficient condition for the existence of a positive semi-definite matrix A with eigenvalues λ_k and diagonal elements a_{kk} is that λ_k majorizes a_{kk}.

Corollary 2. *Let A be a $d \times d$ positive semi-definite matrix with* $\operatorname{Tr} A = 1$. *Then there are d normalized vectors $\mathbf{x}_m$ such that*

$$A = \sum_{m=1}^{d} \tfrac{1}{d} \mathbf{x}_m \mathbf{x}_m^\dagger \tag{8}$$

Proof: Note that any set of non-negative eigenvalues λ_k with $\sum_k \lambda_k = 1$ majorizes the vector $(\frac{1}{d}, \frac{1}{d}, \ldots, \frac{1}{d})$. Therefore, by Horn's lemma, one can find a unitary U and a self-adjoint matrix B such that $A = UB^2U^\dagger$ and the diagonal elements of B^2 are all $\frac{1}{d}$. (In fact, U, B can be chosen to have real elements.) Write $U = \sum_k \mathbf{u}_k \mathbf{e}_k^\dagger$ where $\mathbf{u}_k$ denotes the k-th column of U and $\mathbf{e}_k$ the standards basis. Let $\mathbf{x}_m = \sqrt{d} \sum_j \mathbf{u}_j b_{jm}$. Then

$$\begin{aligned} A &= \sum_{jk} \mathbf{u}_j \langle \mathbf{e}_j B^2 \mathbf{e}_k \rangle \mathbf{u}_k^\dagger \\ &= \sum_{jk} \sum_m \mathbf{u}_j \langle \mathbf{e}_j B \mathbf{e}_m \rangle \langle \mathbf{e}_m, B \mathbf{e}_k \rangle \mathbf{u}_k^\dagger \\ &= \sum_m \tfrac{1}{d} \mathbf{x}_m \mathbf{x}_m^\dagger \end{aligned} \tag{9}$$

[1] See Theorem 4.3.32 of [13]. Note that [12] is by Alfred Horn, but that [13] is co-authored by Roger A. Horn.

and, since the columns of a unitary matrix are orthonormal,

$$\begin{aligned}\|\mathbf{x}_m\|^2 &= d\sum_{jk}\mathbf{u}_j^\dagger \bar{b}_{jm} b_{km}\mathbf{u}_k = d\sum_{jk}\bar{b}_{jm} b_{km}\mathbf{u}_j^\dagger\mathbf{u}_k \\ &= \sum_{jk}\delta_{jk}\bar{b}_{jm}b_{km} = d(B^2)_{mm} = d\tfrac{1}{d} = 1. \qquad \textbf{QED} \end{aligned} \tag{10}$$

This suggests that we restate the conjecture (7) using vectors of block matrices of the form $\mathbf{X}_m^\dagger = \begin{pmatrix} X_{1m}^\dagger & X_{2m}^\dagger & \dots & X_{d_2m}^\dagger\end{pmatrix}$ with each block $d_1 \times d_1$.

Conjecture 5. *Let $\mathbf{A}$ be a d_1d_2 positive semi-definite matrix consisting of $d_2 \times d_2$ blocks A_{jk} each of size $d_1 \times d_1$, with $\sum_j A_{jj} = M$. Then one can find d_2 vectors $\mathbf{X}_m$ composed of d_2 blocks X_{jm} of size $d_1 \times d_1$ such that*

$$\mathbf{A} = \sum_{m=1}^{d_2} \tfrac{1}{d_2}\mathbf{X}_m\mathbf{X}_m^\dagger, \quad \textit{and} \tag{11}$$

$$\sum_k X_{km}X_{km}^\dagger = M \qquad \forall\ m \tag{12}$$

There is no loss of generality in replacing B_m by $\mathbf{X}_m\mathbf{X}_m^\dagger$ with $\mathbf{X}_m$ of the above form. If X is $d_1d_2 \times d_1d_2$ with rank d_1, then by the SVD it can be written as $X = UDV^\dagger$ with U, V unitary and D diagonal with $d_{jj} = 0$ for $j > d$. If $\widetilde{D}$ retains only the first d_1 columns of D, then $\widetilde{X} = U\widetilde{D}$ has the desired form and $\widetilde{X}\widetilde{X}^\dagger = XX^\dagger$. thus, Conjecture 5 is clearly a generalization of Horn's lemma to block matrices.

When $d_2 = 2$, the argument in [24] (due to S. Szarek) is easily extended to give a proof of Conjecture 4 . Then $\mathbf{A} > 0$ is equivalent to

$$\mathbf{A} = \begin{pmatrix}\sqrt{A_{11}} & 0 \\ 0 & \sqrt{A_{22}}\end{pmatrix}\begin{pmatrix} I & W \\ W^\dagger & I\end{pmatrix}\begin{pmatrix}\sqrt{A_{11}} & 0 \\ 0 & \sqrt{A_{22}}\end{pmatrix} \tag{13}$$

with W a contraction. Write the SVD of W as

$$\begin{aligned} W &= U\begin{pmatrix} \cos\theta_1 & 0 & 0 & \dots & 0 \\ 0 & \cos\theta_2 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & \cos\theta_d \end{pmatrix} V^\dagger \\ &= \tfrac{1}{2}U\begin{pmatrix} e^{i\theta_1} & 0 & 0 & \dots & 0 \\ 0 & e^{i\theta_2} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & e^{i\theta_d} \end{pmatrix} V^\dagger + \tfrac{1}{2}U\begin{pmatrix} e^{-i\theta_1} & 0 & 0 & \dots & 0 \\ 0 & e^{-i\theta_2} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & e^{-i\theta_d} \end{pmatrix} V^\dagger \\ &= \tfrac{1}{2}(W_1 + W_2) \end{aligned} \tag{14}$$

with W_1 and W_2 unitary. When W is a $d_1 \times d_1$ unitary, $\begin{pmatrix} I & W \\ W^\dagger & I \end{pmatrix}$ has rank d_1. Therefore, substituting (14) into (13) shows that $\mathbf{A}$ is the midpoint of two matrices with rank at most d_1 and the same blocks on the diagonal as $\mathbf{A}$.

This argument suggests that one might strengthen the conjecture to require that each $\mathbf{B}_m$ have the same diagonal blocks as $\mathbf{A}$. However, this does not appear to hold in the limiting case $d_1 = 1$ with $d_2 > 2$. In the proof of Corollary 2, it is tempting to replace B by $C = BV$ with V unitary. However, in (10) we would obtain $(C^\dagger C)_{mm}$ which, unlike $CC^\dagger$ need not have diagonal elements $\frac{1}{d}$.

The original proof of Horn's lemma used a complicated induction argument based on the properties of augmenting a matrix by a row and column. Since we know that (11) holds when $d_2 = 2$ or $d_1 = 1$, we have the starting points for a (probably non-trivial) double induction argument. Although Audenaert has found extensive numerical evidence for the validity of Conjectures 2-5, a proof seems to be elusive.

3 Depolarized Werner-Holevo channels

The Werner-Holevo channel $\mathcal{W}(\rho) = \frac{1}{d-1}\big((\operatorname{Tr}\rho)\, I - \rho^T\big)$ has been extensively studied, especially in connection with the conjectured mutliplicativity of the maximal output p-norm, defined as $\nu_p(\Phi) = \sup_\rho \|\Phi(\rho)\|_p$. For $d = 3$, the maximal output p-norm is not multiplicative for $p > 4.79$. However, it is known that $\nu_p(\mathcal{W} \otimes (\mathcal{W}) = [\nu_p(\mathcal{W})]^2$ for $1 \leq p \leq 2$. For larger d one obtains a counter-example to multiplicativity only for correspondingly large p. In fact, it has been argued [11] that for $d > 2^p$ the WH channel is multiplicative.

$\mathcal{W}$ maps any pure state $|\psi\rangle\langle\psi|$ to $\frac{1}{d-1}E$ with $E = I - |\psi\rangle\langle\psi|$. Therefore, when d is large, $\mathcal{W}$ behaves much like the completely noisy map (although it is never EB). It is natural to consider channels of the form

$$\Phi_x = x\mathcal{I} + (1-x)\mathcal{W} \tag{15}$$

and ask if they also satisfy the multiplicativity conjecture (23) for $1 \leq p \leq 2$. Channels of the form (15) were considered by Ritter [23] in a different context.

Problem 6. *Show that the channel $\Phi_x = x\mathcal{I} + (1-x)\mathcal{W}$ satisfies the multiplicativity property $\nu_p(\Phi_x \otimes (\Phi_x) = [\nu_p(\Phi_x)]^2$ for $1 \leq p \leq 2$.*

When $d = 3$ and $x = \frac{1}{3}$, the channel (15) becomes

$$\Phi_{1/3}(\rho) = \tfrac{1}{3}\big(I + \rho - \rho^T\big) \tag{16}$$

which has many interesting properties. It seems to have been first considered by Fuchs, Shor and Smolin, who published only an oblique remark at the end of [8]. They wrote it in a very different form, which is also given in [15]. Let $|1\rangle, |2\rangle, |3\rangle$ be an orthonormal basis for $\mathbf{C}_3$ and define

$$\begin{aligned}
|\psi_0\rangle &= 3^{-1/2}\big(|1\rangle + |2\rangle + |3\rangle\big) \\
|\psi_1\rangle &= 3^{-1/2}\big(|1\rangle - |2\rangle - |3\rangle\big) \\
|\psi_2\rangle &= 3^{-1/2}\big(|1\rangle - |2\rangle + |3\rangle\big) \\
|\psi_3\rangle &= 3^{-1/2}\big(|1\rangle + |2\rangle - |3\rangle\big).
\end{aligned}$$

Now let Ψ be the channel whose Kraus operators are $\frac{\sqrt{3}}{2}|\psi_k\rangle\langle\psi_k|$ for $k = 0, 1, 2, 3$. This channel has the following properties:

1. $\Psi = \Phi_{1/3} = \frac{1}{3}\mathcal{I} + \frac{2}{3}\mathcal{W}$. Although this is not obvious, it is easily verified and implies (16). Thus, Ψ maps every real density matrix to the maximally mixed state.

2. Ψ is unital and the Holevo capacity satisfies

$$C_{\text{Hv}}(\Phi) = \log 3 - S_{\min}(\Phi) \tag{17}$$

   but requires 6 (non-orthogonal) input states to achieve this capacity. It is not hard to see that $S_{\min}(\Phi)$ is achieved on inputs which are permutations of $(1, \pm i, 0)^T$.

3. Ψ is an extreme point of the EB channels which is neither CQ nor an extreme point of the CPT maps [15].

A solution of Problem 6 in the case $p = 2$ was recently reported by Michalakis [21].

4 Random sub-unitary channels

The Kraus operators for the WH channels with $d = 3$ can be written as

$$A_k = \tfrac{1}{2}X^k \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad k = 0, 1, 2 \tag{18}$$

where X is the shift operator $X|e_j\rangle = |e_{j+1}\rangle$. This suggests a natural generalization to channels with Kraus operators

$$A_k = \tfrac{1}{2}X^k \begin{pmatrix} u_{11} & u_{12} & 0 \\ u_{21} & u_{22} & 0 \\ 0 & 0 & 0 \end{pmatrix} = \tfrac{1}{2}X^k \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix} \qquad k = 0, 1, 2 \tag{19}$$

with u_{jk} the elements of a 2×2 unitary U. The choice $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ does not give a counterexample to (23), although the effect of a tensor product on a maximally entangled state is the same as the WH channel. This is because changing -1 to $+1$ allows a "purer" optimal output for a single use of the channel; to be precise, for $+1$ the input $\frac{1}{\sqrt{3}}(1,1,1)$ yields an output with eigenvalues $\frac{2}{3}, \frac{1}{6}, \frac{1}{6}$ as compared to eigenvalues $\frac{1}{2}, \frac{1}{2}, 0$ for -1.

By contrast, the standard generalization of the WH channel to $d > 3$ involves $\binom{d}{2}$ choices of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ as the only non-zero block of a $d \times d$ matrix. It would seem natural to study channels with d Kraus operators of the form

$$\tfrac{1}{d-1} X^k \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix} \qquad k = 0, 1, \ldots d-1. \tag{20}$$

where U is a $d-1 \times d-1$ unitary matrix. Such channels are generically extreme and always in the closure $\overline{\mathcal{E}(3,3)}$. Limited attempts to find new counter-examples of this type have found similar behavior to changing $+1$ to -1 does; they have outputs which are "too pure" for a single use of the channel.

Nevertheless, channels with Kraus operators of the form (20) have interesting properties that makes them worth further study. Moreover, it is not necessary to use the same U in every Kraus operator. One can choose

$$A_k = \tfrac{1}{d-1} X^k \begin{pmatrix} U_k & 0 \\ 0 & 0 \end{pmatrix} \qquad k = 0, 1, \ldots d-1. \tag{21}$$

with U_k any set of unitaries in M_{d-1}. With a few exceptions, channels whose Kraus operators have the form (21) are extreme points of the CPT maps on M_3, and are always in $\overline{\mathcal{E}}(3,3)$.

The WH channel gives a counter-example to multiplicativity for large p because maximally entangled states have outputs whose p-norms are relative maxima of $\|(\mathcal{W} \otimes \mathcal{W})(\rho)\|_p$, Nathanson [22] has shown analytically that for any p the output of any maximally entangled state gives a critical point, but Shor has found numerical evidence [28] that this is a relative maximum only for $p \geq 3$. This suggests that one look at other random sub-unitary channels.

Problem 7. *Let Φ be a channel with Kraus operators of the form* (21)*. Does the set of relative maxima of $\|(\Phi \otimes \Phi)(\rho)\|_p$ always include outputs whose input is maximally entangled? If not, for what p and under what circumstances do maximally entangled inputs yield outputs which are relative maxima?*

Moreover, despite the failure of Ruskai's very limited attempt to find new counter-examples of this type for $d = 4, 5$, more extensive numerical investigations, perhaps with different, randomly chosen, U_k, could be worthwhile. Further suggestions about numerical searches are given in Section 5.2. Even a negative result could provide some insight.

Problem 8. *Search for new counterexamples to* (23) *with* Φ *be a channel with Kraus operators of the form* (21)*.*

In addition to looking at the optimal output purity of these channels, one can also ask about their coherent information and quantum capacity.

Problem 9. *What are the properties of the coherent information of random sub-unitary channels? When are they degradable? When is their coherent information additive?*

5 Maximal p-norm multiplicativity

5.1 Additivity and multiplicativity conjectures

One of the outstanding open problems in quantum information is the additivity of minimal output entropy, i.e.,

$$S_{\min}(\Phi \otimes \Omega) = S_{\min}(\Phi) + S_{\min}(\Omega) \tag{22}$$

where $S_{\min}(\Phi) = \inf_{\gamma} S[\Phi(\gamma)$ where the infimum is taken over the set of density matrices γ so that $\gamma > 0$ and $\operatorname{Tr}\gamma = 1$. This conjecture has considerable importance because Shor [27] has shown that it is globablly equivalent to the conjectured additivity of Holevo capacity and several conjectures about entanglement of formation. Shirokov [25, 26] has even shown that additivity in all finite dimensions would have implications for certain infinite dimensional channels. Fukuda [9] and Wolf [10] have given some additional reductions.

Amosov, Holevo and Werner [1] realized that (22) would follow if the following conjecture holds for $p \in (1, 1+\epsilon)$ with $\epsilon > 0$.

$$\nu_p(\Phi \otimes \Omega) = \nu_p(\Phi)\nu_p(\Omega) \tag{23}$$

where $\nu_p(\Phi) = \inf_{\gamma} \|\Phi(\gamma)\|_p$. Although, Werner and Holevo [29] found a counter-example to (23) for large p, it seems reasonable to conjecture that (23) holds for $1 \leq p \leq 2$.

5.2 Finding counter-examples

It is surprising that no counter-example to (23) is known other than the WH channel [29] and very small perturbations of it. Moreover, one has no counter-example for

$p < 4.79$. Some authors [18] have conjectured that (23) holds for $1 \leq p \leq 2$. If so, one would expect to have a family of counter-examples for $p > 2$. More generally, if the conjecture hold for $1 < p < p_c$, one would expect to find counter-examples for $p > p_c$ arbitrarily close to to p_c.

Problem 10. *Find more counter-examples to* (23)*. Do they suggest that the conjecture holds for* $1 \leq p \leq 2$*?*

One strategy for finding new counter-examples, is to first search numerically for additional counter-examples for very *large* p using Theorem 3 below. For any new examples found, study the critical points numerically and determine the values of p for which one ceases to have a counter-example and for which one ceases to even have a relative maximum for entangled inputs. Perhaps this will give some insight into the nature of counter-examples that will allow one to find some in the range $2 < p < 4.79$. The reason for starting with large p is that the algorithm for finding relative maxima using Theorem 3 is faster and more robust for large p.

The following extension of Shor algorithm for finding relative minima of the minimal ouput entropy (see Appendix of [6]) is due to C. King.

Theorem 3. (King-Shor) *Let* Ω *be a CPT map and* $\widehat{\Omega}$ *its adjoint with respect to the Hilbert-Schmidt inner product. For fixed* $\rho = |\psi_0\rangle\langle\psi_0|$*, let* ψ_1 *be the eigenvector corresponding to the largest eigenvalue of* $\widehat{\Omega}\big[\Omega(\rho)\big]^{p-1}$*. Then* $\|\Omega(|\psi_1\rangle\langle\psi_1|)\|_p > \|\Omega(\psi_0)\|_p$

Proof: By the max min principle,

$$\langle\psi_1\widehat{\Omega}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^{p-1}\psi\rangle \geq \langle\psi_0\widehat{\Omega}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^{p-1}\psi_0\rangle. \tag{24}$$

Then Hölder's inequality implies

$$\begin{aligned} \mathrm{Tr}\,\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^p &\leq \mathrm{Tr}\,\big[\Omega\big(|\psi_1\rangle\langle\psi_1|\big)\big]\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^{p-1} \\ &\leq \Big[\mathrm{Tr}\,\big[\Omega\big(|\psi_1\rangle\langle\psi_1|\big)\big]^p\Big]^{1/p}\Big[\mathrm{Tr}\,\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^p\Big]^{1-1/p} \end{aligned} \tag{25}$$

which gives

$$\Big(\mathrm{Tr}\,\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^p\Big)^{1/p} \leq \Big(\mathrm{Tr}\,\big[\Omega\big(|\psi_1\rangle\langle\psi_1|\big)\big]^p\Big)^{1/p} \tag{26}$$

or, equivalently,

$$\|\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\|_p \leq \|\Omega\big(|\psi_1\rangle\langle\psi_1|\big)\|_p. \qquad \textbf{QED} \tag{27}$$

Using this result repeatedly with ψ_{k+1} the eigenvector corresponding to the largest eigenvalue of $\widehat{\Omega}\big[\Omega(|\psi_k\rangle\langle\psi_k|)\big]^{p-1}$, gives a sequence converging to a relative maximum of $\|\Phi(\rho)\|_p$.

Remarks on critical points.

5.3 Specific multiplicativity problems

Proving multiplicativity of the depolarized WH channel was already mentioned as an open problem in Section 3. Recently, Michalakis reported [21] a proof for $p = 2$. In view of the fact that some depolarized WH channels do *not* satisfy the very unappealing conditions based on positive entries used in [18, 16], this suggests that one revisit the general case of $p = 2$.

Problem 11. *Prove* (23) *for* $p = 2$ *and arbitrary CPT maps.*

In [22], a class of channels is defined using mutually unbiased bases, with each basis defining an "axis". These channels can be described by "multipliers" in a manner similar to unital qubits channels, and when all multipliers are non-negative they seem very similar. However, even for a single use of a channel some questions are open. See Conjecture 9 of [22]. If this conjecture is true, then additivity and multiplicativity can be reduced to the case of "maximally squashed" channels which are generalizations of the two-Pauli qubit channel.

Problem 12. *Find a proof of multiplicativity for the two-Pauli qubit channel, which does not use unitary equivalence to channels with negative multipliers.*

5.4 Reduction to extreme points

Although the set of CPT maps $\Phi : M_{d_A} \mapsto M_{d_B}$ is convex, one can not use convexity to reduce additivity or multiplicativity to that of the extreme channels. One can, however, use the notion of complementary channels to obtain a kind of global reduction to extreme channels.

The notion of complementary channel was first used in quantum information theory in a paper of Devetak and Shor [7] and then studied in detail in [14, 17]. This channel is equivalent to one obtained much earlier in a more general context by Arveson [2] by his commutant lifting theorem.

If $\Phi : M_{d_A} \mapsto M_{d_B}$, its complement is a CPT map $\Phi^C : M_{d_A} \mapsto M_{d_E}$ with Choi rank d_B. Whenever $d_B \leq d_A$, the complement belongs to the class of generalized extreme points. Therefore, by the results in [14, 17] if we can prove additivity or multiplicativity for all maps in $\overline{\mathcal{E}(d_1, d_2)}$, it will hold for all CPT maps with $d_B \leq d_A$. Moreover, Shor's channel extensions [27] used to establish the equivalence of various additivity results increase only d_A. Hence, additivity for tensor products of all extreme maps with $d_A \geq d_B$ would imply it for all maps with $d_A = d_B$.

Problem 13. *Identify new classes of extreme CPT maps for which multiplicativity can be proved.*

Problem 14. *Prove* (23) *for random sub-unitary channels, at least for* $p = 2$.

5.5 Coherent information and degradability

In the note [5] on degradability, the following question was raised.

Problem 15. *When are pairs of channels $\mathcal{M}, \mathcal{N}$ mutually degradable in the sense that there exist channels $\mathcal{X}, \mathcal{Y}$ such that*

$$\mathcal{X} \circ \mathcal{M} = \mathcal{N}^C \qquad \mathcal{Y} \circ \mathcal{N} = \mathcal{M}^C. \tag{28}$$

At present, the only examples known have $\mathcal{M} = \mathcal{I}$ which is universal in the sense that $\mathcal{N}$ is arbitrary. This works because $\mathcal{I}$ is universally degradable and its complement Tr is a universal degrador. Can other examples be found?

6 Local invariants for N-representability

In the 1960's a variant of the quantum marginal problem known as N-representability attracted considerable interest. The question is to find necessary and sufficient conditions on a p-particle reduced density matrix $\rho_{1,2,\ldots t}$ in order that there exists an anti-symmetric (or symmetric for bosons) N-particle density matrix $\rho = \rho_{1,2\ldots N}$ such that $\mathrm{Tr}_{t+1,t+2,\ldots N}\rho_{1,2\ldots N} = \rho_{1,2,\ldots t}$. The pure N-representability problem, for which one requires that the preimage $\rho_{1,2\ldots N} = |\Psi\rangle\langle\Psi|$ come from an anti-symmetric (or symmetric) pure state $|\Psi\rangle$ is also of interest.

A full solution was found only to the mixed state problem for the one-particle density matrix, for which it is necessary and sufficient that the eigenvalues of ρ_1 are $\leq \frac{1}{N}$ when $\mathrm{Tr}\,\rho_1 = 1$. Other results were obtained for a few very special situations, and some reformulations were found. For the two-particle reduced density matrix, a collection of necessary inequalities were obtained, but little else was known. For over 30 years, there was very little progress until two recent breakthroughs. Klyachko [19] solved the pure state 1-representability problems. Liu, Christandl and Verstraete [20] showed that some version are QMA complete.

Although many open questions remain, we consider only one which may be amenable to quantum information theorists. As Coleman pointed out, N-representability must be independent of the 1-particle basis used to write the density matrix, i.e., the solution can be expressed in terms of what one might call local invariants. These are parameters which are invariant under transformations of the form $U \otimes U \otimes \ldots \otimes U = U^{\otimes p}$. For the 1-matrix, these are just unitary invariants, which are known to be the eigenvalues. For $p = 2$ the set of local invariants includes the eigenvalues, but must contain other parameters as well. Surprisingly, no complete set of local invariants in which N-representability conditions for the 2-matrix can be expressed is known.

Problem 16. *Find a minimal complete set of local invariants for an anti-symmetric (or symmetric) 2-particle density matrix.*

References

[1]

[2] W. Arveson

[3] M-D Choi, "Completely Positive Linear Maps on Complex Matrices" *Lin. Alg. Appl.* **10**, 285–290 (1975).

[4] A.J. Coleman, "The structure of fermion density matrices" *Rev. Mod. Phys.* **35**, 668–687 (1958).

[5] T. Cubbit, M.B. Ruskai and G. Smith

[6] N. Datta and M.B. Ruskai

[7] I. Devetak and P. Shor

[8] C. Fuchs, "Nonorthogonal quantum states maximize classical information capacity", *Phys. Rev. Lett.* **79**, 1162–1165 (1997).

[9] M. Fukuda

[10] M. Fukuda and M.M. Wolf

[11] V. Giovannetti, S. Lloyd and M. B. Ruskai, "Conditions for multiplicativity of maximal l_p-norms of channels for fixed integer p", *J. Math. Phys.* **46**, 042105 (2005). quant-ph/0408103.

[12] A. Horn,

[13] R.A. Horn and C.R. Johnson, *Matrix Analysis* (Cambridge University press, 1985).

[14] A. S. Holevo, "On complementary channels and the additivity problem" quant-ph/0509101

[15] M.Horodecki, P. Shor, and M. B. Ruskai "Entanglement Breaking Channels" *Rev. Math. Phys* **15**, 629–641 (2003). (quant-ph/030203)

[16] C. King, M. Nathanson and M. B. Ruskai,

[17] C. King, K. Matsumoto, M. Nathanson and M. B. Ruskai, "Properties of Conjugate Channels with Applications to Additivity and Multiplicativity" (quant-ph/0509126.

[18] C. King and M.B. Ruskai

[19] A. Klyachko, "Quantum marginal problem and N-representability" *Journal of Physics: Conf. Series* **36**, 72–86 (2006). quant-ph/0511102

[20] Y.-K. Liu, M. Christandl, F. Verstraete "N-representability is QMA-complete" quant-ph/0609125

[21] S. Michalakis, private communication.

[22] M. Nathanson and M.B. Ruskai "Pauli Diagonal Channels Constant on Axes" quant-ph/0611106

[23] G. W. Ritter, "Quantum Channels and Representation Theory" *J. Math. Phys.* **46**, (2005) (quant-ph/0502153).

[24] M. B. Ruskai, S. Szarek, E. Werner, "An analysis of completely positive trace-preserving maps M_2" *Lin. Alg. Appl.* **347**, 159 (2002).

[25] Shirokov

[26] Shirokov

[27] P. W. Shor, "Equivalence of Additivity Questions in Quantum Information Theory", *Commun. Math. Phys.* **246**, 453–472 (2004). quant-ph/0305035

[28] P. W. Shor, private communication. This result has been confirmed by M. Nathanson.

[29] R. F. Werner and A. S. Holevo, "Counterexample to an additivity conjecture for output purity of quantum channels", *J. Math. Phys.* **43**, 4353–4357 (2002).