Reviews in Mathematical Physics
Vol. 15, No. 6 (2003) 629–641

World Scientific
www.worldscientific.com

ENTANGLEMENT BREAKING CHANNELS

MICHAEL HORODECKI

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
fizmh@univ.gda.pl

PETER W. SHOR

AT&T Labs Research, Florham Park, New Jersey 07922 USA
shor@research.att.com

MARY BETH RUSKAI

Department of Mathematics, Tufts University, Medford, Massachusetts 02155 USA
marybeth.ruskai@tufts.edu

Received 2 February 2003
Revised 30 May 2003

This paper studies the class of stochastic maps, or channels, for which $(I \otimes \Phi)(\Gamma)$ is always separable (even for entangled Γ). Such maps are called entanglement breaking, and can always be written in the form $\Phi(\rho) = \sum_k R_k \operatorname{Tr} F_k \rho$ where each R_k is a density matrix and $F_k > 0$. If, in addition, Φ is trace-preserving, the $\{F_k\}$ must form a positive operator valued measure (POVM). Some special classes of these maps are considered and other characterizations given.

Since the set of entanglement-breaking trace-preserving maps is convex, it can be characterized by its extreme points. The only extreme points of the set of completely positive trace preserving maps which are also entanglement breaking are those known as classical-quantum or CQ. However, for $d \geq 3$, the set of entanglement breaking maps has additional extreme points which are not extreme CQ maps.

Keywords: Quantum channels; entanglement breaking maps; completely positive maps; CQ channels; separable states; extreme points.

1. Introduction

A quantum channel is represented by a stochastic map, i.e. a map which is both completely positive and trace-preserving. We will refer to these as CPT maps. In this paper we consider the special class of quantum channels which can be simulated by a classical channel in the following sense: The sender makes a measurement on the input state ρ, and sends the outcome k via a classical channel to the receiver who

then prepares an agreed upon state R_k. Such channels can be written in the form

$$\Phi(\rho) = \sum_k R_k \operatorname{Tr} F_k \rho \tag{1}$$

where each R_k is a density matrix and the $\{F_k\}$ form a positive operator valued measure (POVM). We call this the "Holevo form" because it was introduced by Holevo in [6].

It is also natural consider the class of channels which break entanglement.

Definition 1. *A stochastic map* Φ *is called* entanglement breaking *if* $(I \otimes \Phi)(\Gamma)$ *is always separable, i.e. any entangled density matrix* Γ *is mapped to a separable one.*

It is not hard to see that, as shown in the next section, a map is entanglement-breaking if and only if it can be written in the form

$$\Phi(\rho) = \sum_k |\psi_k\rangle\langle\psi_k| \langle\phi_k, \rho\phi_k\rangle \tag{2}$$

in which case it is necessarily completely positive. Furthermore, Φ is trace-preserving if and only if $\sum_k |\phi_k\rangle\langle\phi_k| = I$, in which case, (2) is a special case of (1). One can show that the converse also holds, so that we have the following result.

Theorem 2. *A channel can be written in the form* (1) *using positive semi-definite operators* F_k *if and only if it is entanglement breaking. Such a map is also trace-preserving if and only if the* $\{F_k\}$ *form a POVM or, equivalently,* $\sum_k |\phi_k\rangle\langle\phi_k| = I$.

The rather straightforward proof will be given in the next section together with some additional equivalences. We will refer to stochastic maps which are both entanglement-breaking and trace-preserving as EBT.

Of course there are stochastic maps which are not of the form (1). In particular, conjugation with a unitary matrix is not EBT. Channels which break entanglement are particularly noisy in some sense, e.g. a qubit map is EBT if the image of the Bloch sphere collapses to a plane or a line. In the opposite direction, we will show that a channel in d dimensions is *not* EBT if it can be written using fewer than d Kraus operators.

Theorem 3. *The set of EBT maps is convex.*

Although this follows easily from the definition of entanglement breaking, it may be instructive to also show directly that the set of maps of the form (1) is convex. Let Φ and $\tilde{\Phi}$ denote such maps with density matrices $\{R_j\}_{j=1\cdots m}$ and $\{\tilde{R}_k\}_{k=1\cdots n}$ and POVM's $\{E_j\}_{j=1\cdots m}$ and $\{\tilde{E}_k\}_{k=1\cdots n}$ respectively. For any $\alpha \in [0,1]$ the map

$$[\alpha\Phi + (1-\alpha)\tilde{\Phi}](\rho) = \sum_j R_j \operatorname{Tr}(\alpha E_j \rho) + \sum_k \tilde{R}_k \operatorname{Tr}[(1-\alpha)\tilde{E}_j \rho]$$

has the form (1) since $\{\alpha E_1, \alpha E_2, \ldots, \alpha E_m, (1-\alpha)\tilde{E}_1, \ldots, (1-\alpha)\tilde{E}_n\}$ is also a POVM.

Note that we have used implicitly the idea of generating a new POVM as the convex combination of two POVM's, In this sense, the set of POVM's is also convex, and one might expect that the extreme points of the set of entanglement-breaking maps are precisely those with an extreme POVM and pure R_k. However, this is false; at end of Sec. 3 of [18], the trine POVM is used to give an example of a qubit channel which is not extreme, despite the fact that the POVM is.

Certain subclasses of EBT maps are particularly important. Holevo called a channel

- *classical-quantum* (CQ) if each $F_k = |k\rangle\langle k|$ in the POVM is a one-dimensional projection. In this case, (1) reduces to $\Phi(\rho) = \sum_k R_k \langle k, \rho k\rangle$.
- *quantum-classical* (QC) if each density matrix $R_k = |k\rangle\langle k|$ is a one-dimensional projection and $\sum_k R_k = I$.

If a CQ map has the property that each density matrix $R_k = |\psi_k\rangle\langle\psi_k|$ is a pure state, we will call it an *extreme CQ* map. Note that the pure states $|\psi_k\rangle$ need not be orthonormal, or even linearly independent. We will see in Sec. 3 that extreme CQ maps are always extreme points of the set of EBT maps, but they are only extreme points for the set of CPT maps if all pairs $\langle\psi_j, \psi_k\rangle$ are nonzero.

When all $R_k = R$ are identical, then Φ is the maximally noisy map $\Phi(\rho) = R$ for all ρ. Because it maps all density matrices to the same R, its image is a single "point" in the set of density matrices and its capacity is zero. A point channel is extreme if and only if its image R is a pure state. A *point* channel is a special case of a CQ map; however, because all $R_k = R$ the sum in (1) can be reduced to a single term with $E_1 = I$. For $d > 2$, one can also consider those CQ maps for which some R_k are identical; then the POVM can be written as a projective measurement, and the image is a polyhedron.

It is useful to have Kraus operator representations of EBT maps. For Φ of the form (1), let $A_{kmn} = \sqrt{R_k}|m\rangle\langle n|\sqrt{F_k}$ where $\{|m\rangle\}$ and $\{|n\rangle\}$ are orthonormal bases. Then one easily verifies that

$$\sum_{kmn} A_{kmn}\rho A_{kmn}^\dagger = \sum_k R_k \operatorname{Tr} F_k \rho\,. \tag{3}$$

For CQ and QC maps these operators reduce to $A_{km} = \sqrt{R_k}|m\rangle\langle k|$ and $A_{kn} = |k\rangle\langle n|\sqrt{F_k}$ respectively. Moreover, if all density matrices are pure states $R_k = |\psi_k\rangle\langle\psi_k|$, then one can achieve a further reduction to $A_k = |\psi_k\rangle\langle k|$ in the case of CQ maps.

Holevo [6] showed that for EBT maps the Holevo capacity (i.e. the capacity of a quantum channel used for classical communication with product inputs) is additive. This result was extended by King [13] to additivity of the capacity of channels of the form $\Phi \otimes \Omega$ where Φ is CQ or QC and Ω is completely arbitrary. Shor [20] then proved the additivity of minimal entropy and Holevo capacity when Φ is EBT and

Ω arbitrary. Quite recently, King [14] showed that the maximal p-norms of EBT channels are multiplicative, and used this to give another proof of Shor's additivity results for minimal entropy and Holevo capacity. In a related development, Vidal, Dür and Cirac [22] used Shor's techniques to prove additivity of the entanglement of formation for a class of mixed states associated with EBT maps.

As it is important to understand the differences between those channels which break entanglement and those which preserve it, we seek other characterizations of these channels, describe their extreme points, and examine their properties. Results for qubits are given in a related paper [18] which follows. Some analysis of entanglement breaking channels was also independently presented by Verstraete and Verschelde [21].

2. Equivalent Conditions

In this section, we establish a number of equivalent characterizations of EBT maps, some of which were already discussed in the previous section.

Theorem 4. *The following are equivalent*

(A) Φ *has the Holevo form* (1) *with* F_k *positive semi-definite.*
(B) Φ *is entanglement breaking.*
(C) $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ *is separable for* $|\beta\rangle = d^{-1/2} \sum_j |j\rangle \otimes |j\rangle$ *a maximally entangled state.*
(D) Φ *can be written in operator sum form using only Kraus operators of rank one.*
(E) $\Upsilon \circ \Phi$ *is completely positive for all positivity preserving maps* Υ.
(F) $\Phi \circ \Upsilon$ *is completely positive for all positivity preserving maps* Υ.

A corresponding equivalence holds for CPT and EBT maps with the additional conditions that $\{F_k\}$ *is a POVM, the Kraus operators* A_k *satisfy* $\sum_k A_k^\dagger A_k = I$, *and* Υ *is trace-preserving.*

To prove this result, we will make use of the correspondence [2, 12] between maps and states given by $\Phi \leftrightarrow (I \otimes \Phi)(|\beta\rangle\langle\beta|)$. (Also see [1] in this context.)

Proof. To show that (A) $\Rightarrow$ (B) note that when Φ has the form (1),

$$(I \otimes \Phi)(\Gamma) = \sum_k R_k T_2(\sqrt{E_k}\,\Gamma\sqrt{E_k})$$

$$= \sum_k \gamma_k R_k \otimes Q_k$$

where T_2 denotes the partial trace, $\gamma_k = \operatorname{Tr} E_k\Gamma$ and $Q_k = \frac{1}{\gamma_l} T_2(\sqrt{E_k}\Gamma\sqrt{E_k})$. Thus, for arbitrary Γ, $(I \otimes \Phi)(\Gamma)$ is separable.

The implication (B) $\Rightarrow$ (C) is trivial. To see that (C) $\Rightarrow$ (A), observe that since $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ is separable, one can find normalized vectors $|v_n\rangle$ and $|w_n\rangle$

for which

$$(I \otimes \Phi)(|\beta\rangle\langle\beta|) \equiv \frac{1}{d}\sum_{jk} |j\rangle\langle k| \otimes \Phi(|j\rangle\langle k|) \tag{4}$$

$$= \sum_n p_n |v_n\rangle\langle v_n| \otimes |w_n\rangle\langle w_n| \,. \tag{5}$$

Now let Ω be the map

$$\Omega(\rho) = d\sum_n |w_n\rangle\langle w_n| \,\mathrm{Tr}(\rho p_n |v_n\rangle\langle v_n|) \,. \tag{6}$$

Then one easily verifies that

$$(I \otimes \Omega)(|\beta\rangle\langle\beta|) = \sum_{jkn} |j\rangle\langle k| \otimes |w_n\rangle\langle w_n| p_n \langle j, v_n\rangle\langle v_n, k\rangle$$

$$= \sum_n p_n |v_n\rangle\langle v_n| \otimes |w_n\rangle\langle w_n|$$

where we have used $|v_n\rangle = \sum_j |j\rangle\langle j, v_n\rangle$. Since a map Φ is uniquely determined by its action on the basis $|j\rangle\langle k|$, and hence by the action of $(I \otimes \Phi)$ on $|\beta\rangle\langle\beta|$, we can conclude that $\Phi = \Omega$. For trace-preserving maps, we also need to verify that $\{d\, p_n |v_n\rangle\langle v_n|\}$ is a POVM. Taking the partial trace of (5), and using the fact that Φ is trace-preserving yields

$$T_2[(I \otimes \Phi)(|\beta\rangle\langle\beta|)] = \frac{1}{d}\sum_{jk} |j\rangle\langle k| \otimes \mathrm{Tr}(|j\rangle\langle k|) = \frac{1}{d} I$$

$$= \sum_n p_n |v_n\rangle\langle v_n|$$

which is the desired result. Moreover, we have also shown that (C) $\Rightarrow$ (D).

To show that (D) $\Rightarrow$ (A), suppose that $\Phi(\rho) = \sum_k A_k \rho A_k^\dagger$ with $A_k = |w_k\rangle\langle u_k|$. Then the map Φ can be written in the form (1) with $R_k = |u_k\rangle\langle u_k|$. Moreover, when $\sum_k A_k^\dagger A_k = I$, then $\sum_k |u_k\rangle\langle u_k| = I$ so that $F_k = |u_k\rangle\langle u_k|$ defines a POVM.

The equivalence of (E) and (B) follows easily from the fact that a density matrix Γ is separable if and only if $(I \otimes \Omega)(\Gamma) > 0$ for all positivity preserving maps Ω [7]. To see that this is equivalent to (F), it suffices to observe that Ω is positivity preserving if and only if its adjoint $\hat{\Omega}$ is and that $\widehat{\Phi \circ \Upsilon} = \hat{\Upsilon} \circ \hat{\Phi}$, where the adjoint is taken with respect to the Hilbert Schmidt inner product so that $\mathrm{Tr}[\hat{\Omega}(A)]^\dagger B = \mathrm{Tr}\, A^\dagger \Omega(B)$.

It may be interesting to recall that Υ is trace-preserving if and only if $\hat{\Upsilon}$ is unital so that the adjoint of a positivity and trace preserving map preserves POVM's. Thus, when Φ has the form (1), the map $\Phi \circ \Upsilon$ is achieved by replacing E_k by $\hat{\Upsilon}(E_k)$.

Conditions (E) and (F) could be weakened slightly since it would suffice to check either for all Υ in some set of entanglement witnesses for the space on which Φ acts. However, one does not expect to be able to weaken them beyond this. Indeed, [5] and [9] contain examples of a channels which preserve PPT entanglement,

but break other types, i.e. the channel output $(I \otimes \Phi)(\Gamma)$ is entangled, yet the partial transpose $(I \otimes T)$ acting on it always yields a positive semi-definite state $(I \otimes T \circ \Phi)(\Gamma) \geq 0$.

Alternatively, one could also consider maps which are not EBT, but break particular types of entanglement. □

3. Extreme Points

We now give some results about the extreme points of the convex set of EBT maps. In this section we will use some additional results from Choi [2] who observed that Φ is completely positive if and only if $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ is positive semi-definite. When Φ is written in the operator sum form

$$\Phi(\rho) = \sum_k A_k \rho A_k^\dagger \tag{7}$$

the Kraus operators A_k can be chosen as the eigenvectors of $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ with strictly positive (i.e. nonzero) eigenvalue. (See Leung [16] for an nice exposition.) Choi [2] also showed that Φ is extreme in the set of CPT maps if and only if the set $\{A_j^\dagger A_k\}$ is linearly independent. Since both (7) and this linear independence are preserved when $A_i \mapsto \sum_j u_{ij} A_j$, a sufficient condition for Φ to be an extreme EBT map is that $\{A_j^\dagger A_k\}$ is linearly independent for some set of operators $\{A_k\}$ satisfying (7). Note that the condition that Φ is also trace-preserving becomes $\sum_k A_k^\dagger A_k = I$.

Recall that an *extreme CQ map* is one which can be written in the form

$$\Phi(\rho) = \sum_k |\psi_k\rangle\langle\psi_k|\langle e_k, \rho e_k\rangle \tag{8}$$

with the vectors $\{e_k\}$ orthonormal. We can summarize our results as follows.

Theorem 5.

(A) *If Φ is an extreme CQ map, then Φ is an extreme point in the set of EBT maps.*
(B) *If Φ is an extreme CQ map, then Φ is an extreme point in the set of CPT maps if and only if $\langle\psi_j, \psi_k\rangle \neq 0 \ \forall \ j, k$ when it is written in the form* (8).
(C) *If Φ is both in the set of EBT maps and an extreme point of the CPT maps, then Φ is an extreme CQ map.*
(D) *When $d = 2$, the extreme points of the set of EBT maps are precisely the extreme CQ maps. When $d \geq 3$ there are extreme EBT maps which are not CQ.*

Proof. To prove (A) we assume that $\Phi = a\Phi_1 + (1-a)\Phi_2$ with Φ_1, $\Phi_2 \neq \Phi$, $0 < a < 1$ and Φ_1, Φ_2 both EBT. Both Φ_1, Φ_2 can be written in the form (2). By combining these, one finds one can write

$$\Phi(\rho) = \sum_j t_j |\phi_j\rangle\langle\phi_j|\langle f_j, \rho f_j\rangle \tag{9}$$

with Φ_1, Φ_2 having the same form, but different $t_j \geq 0$. By assumption, Φ can be written in the form (8) with $|e_k\rangle$ orthonormal so that

$$\Phi(|e_k\rangle\langle e_k|) = |\psi_k\rangle\langle\psi_k| = \sum_j t_j |\langle e_k, f_j\rangle|^2 |\phi_j\rangle\langle\phi_j| \,. \tag{10}$$

Since all $t_j \geq 0$, the rank one projection $|\psi_k\rangle\langle\psi_k|$ is a linear combination with non-negative coefficients of the projections $|\phi_j\rangle\langle\phi_j|$. This is possible only if those projections $|\phi_j\rangle\langle\phi_j|$ which have nonzero coefficients in (10) are identical to the projection $|\psi_k\rangle\langle\psi_k|$. Hence, we can conclude that every projection $|\phi_j\rangle\langle\phi_j|$ in (9) is equal to one of the projections $|\psi_k\rangle\langle\psi_k|$ in (8). Let us now relabel the projections $|\psi_{k'}\rangle\langle\psi_{k'}|$ so that they are all distinct and let $E_{k'} = \sum_{i\in k'} |e_i\rangle\langle e_i|$ where the sum is taken over those e_i for which the associated projection in (8) is $|\psi_{k'}\rangle\langle\psi_{k'}|$. Then $\{E_{k'}\}$ gives a partition of I into mutually orthogonal projections, i.e. a von Neumann measurement, and we can write (dropping the $'$s for simplicity)

$$\Phi(\rho) = \sum_k |\psi_k\rangle\langle\psi_k| \operatorname{Tr} E_k \rho \,. \tag{11}$$

We can also write

$$\Phi_1(\rho) = \sum_k |\psi_k\rangle\langle\psi_k| \operatorname{Tr} F_k \rho \tag{12}$$

$$\Phi_2(\rho) = \sum_k |\psi_k\rangle\langle\psi_k| \operatorname{Tr} G_k \rho \tag{13}$$

with $\{F_k\}$ and $\{G_k\}$ each a POVM. Since the $|\psi_{k'}\rangle\langle\psi_{k'}|$ were chosen to be distinct and the $E_{k'}$ orthonormal, it follows that $\Phi = a\Phi_1 + (1-a)\Phi_2$ if and only if $E_k = aF_k + (1-a)G_k$. Since $0 \leq F_k, G_k \leq I$, this is possible only if $F_k = G_k = E_k$. But then we have shown that $\Phi_1 = \Phi_2 = \Phi$, which proves part (A).

To prove (B) note that the Kraus operators can be chosen as $A_k = |\psi_k\rangle\langle v_k|$. Thus, $A_j^\dagger A_k = \langle\psi_j, \psi_k\rangle |e_k\rangle\langle e_j|$ which yields a linearly independent set if and only if *none* of the ψ_j are mutually orthogonal. But this is precisely Choi's condition for the map to be extreme in the set of all CPT maps.

The proof of part (C) requires Lemma 8 which is of interest in its own right. The proof of (D) when $d = 2$ is given in the following paper [18] on qubit EBT maps, while the counter-example establishing (D) for $d > 3$ is given below. □

Remark. Recall that a QC map can be written in the form

$$\Phi(\rho) = \sum_k |e_k\rangle\langle e_k| \operatorname{Tr} \rho F_k \tag{14}$$

with the vectors $\{e_k\}$ orthonormal. Such maps can never be extreme in the set of CPT maps; their Kraus operators always include a subset of the form $A_k = |e_k\rangle\langle v_k| G_k$ which can *not* satisfy Choi's linear independence condition due to the orthogonality of the $\{e_k\}$. In the case of qubits, QC maps are not even extreme

in EBT, unless they are also CQ. However, for $d = 4$, one can have extreme EBT maps which are QC but not CQ.

Example. Let $\{g_k\}$ be orthonormal and consider the POVM consisting of a "trine" on span$\{g_1, g_2\}$ and the projection onto span$\{g_3, g_4\}$, i.e.

$$E_1 = \frac{2}{3}|g_1\rangle\langle g_1|\,, \quad E_2 = \frac{2}{3}|g_+\rangle\langle g_+|\,, \quad E_3 = \frac{2}{3}|g_+\rangle\langle g_+|\,, \quad E_4 = |g_3\rangle\langle g_3| + |g_4\rangle\langle g_4|$$

where $|g_\pm\rangle = \frac{1}{2}|g_1\rangle \pm \frac{\sqrt{3}}{2}|g_2\rangle$. Then $\Phi(\rho) = \sum_{k=1}^4 |e_k\rangle\langle e_k| \operatorname{Tr} \rho E_k$ is an extreme EBT map, which is QC, but not CQ.

To see that Φ is extreme it suffices to observe that it is essentially the direct sum of maps $\Phi_A \oplus \Phi_B$ where $\Phi_A : \mathbf{C}^2 \mapsto \mathbf{C}^3$ with $\Phi_A(\rho) = \sum_{k=1}^3 |e_k\rangle\langle e_k| \operatorname{Tr} \rho E_k$ and $\Phi_B : \mathbf{C}^2 \mapsto \mathbf{C}^1$ with $\Phi_B(\rho) = |e_4\rangle\langle e_4|$ for all ρ. Φ_A is extreme because it is the adjoint of an extreme CQ map, and Φ_B is the only CPT from map $\mathbf{C}^2$ to $\mathbf{C}^1$. We used the fact that proof of part (A) of Theorem 5 extends easily to map from $\mathbf{C}^d$ to $\mathbf{C}^{d'}$ with $d' < d$.

A map which is both CQ and QC projects a density matrix ρ onto its diagonal in a fixed orthonormal basis. One can generalize this to CPT maps which take a density matrix to its projection onto a block-diagonal one. Such maps have the form $\Phi(\rho) = \sum_k E_k \rho E_k$ where E_k are the projections in a von Neumann measurement; they are not EBT when at least one of the projections has rank > 1. The map in the example above is a generalization of CQ in the sense that it is the composition of a block diagonal projection together with an EBT map, and thus could be regarded as "block CQ". In a similar spirit, one might regard an extreme CQ map for which the ψ_k can be split into two mutually orthogonal subsets as "block QC". With respect to CPT, maps which are both block QC and block CQ could be considered as generalizations of the quasi-extreme points introduced in [19] for stochastic maps on $\mathbf{C}^2$.

We now give some results about the number of Kraus operators associated with EBT maps.

Theorem 6. *If a CPT map Φ can be written with fewer than d Kraus operators, then it is* not *EBT.*

Proof. This follows from the fact [2] that Φ can always be written using at most $r \equiv \operatorname{rank}[(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ Kraus operators. However, it was shown in [11] that if $r < d$, then $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ is *not* separable and, hence, Φ does not break the entanglement of the state $|\beta\rangle\langle\beta|$. Alternatively, one could observe that if $r < d$, then at least one eigenvalue of $(I \otimes \Phi)(|\beta\rangle\langle\beta|$ is greater than $1/d$, while its left reduced density matrix has all eigenvalues equal to $1/d$ (since Φ is CPT). However, in Ref. 8 it was shown that if a state is separable, then its the maximal eigenvalue must not exceed the maximal eigenvalue of either of subsystems. □

Lemma 7. *If Φ is a CPT map for which* $\operatorname{rank}[(I \otimes \Phi)(|\beta\rangle\langle\beta|)] = d$, *then Φ is EBT if and only if $T \circ \Phi$ is completely positive.*

This follows immediately from a (non-trivial) result in [10] which implies that a $d^2 \times d^2$ density matrix of rank d is separable if and only if it has positive partial transpose.

The following lemma is of some interest since one can find examples [4] of separable matrices of rank d whose decomposition into product pure states requires more than d products. The additional hypothesis that the reduced density matrix $\rho_A = \mathrm{Tr}_B \rho$ also has rank d is crucial. The lemma was first proven in [10]. Here we present a simpler proof.

Lemma 8. *Let ρ be a density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. If ρ is separable, ρ has rank d, and $\rho_A = \mathrm{Tr}_B \rho$ has rank d, then ρ can be written as a convex combination of products of pure states using at most d products.*

Proof. Since ρ is separable it can be written in the form

$$\rho = \sum_{i=1}^{k} \lambda_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i| \,. \tag{15}$$

Assume that $k > d$ and that ρ cannot be written in the form (15) using less than k products. Since ρ_A has exactly rank d, there is no loss of generality in assuming that the vectors above have been chosen so that $|a_1\rangle$, $|a_2\rangle, \ldots, |a_d\rangle$ are linearly independent. Moreover, since ρ has rank $d < k$, the first $d+1$ vectors $|a_i\rangle \otimes |b_i\rangle$ must be linearly dependent so that one can find α_j such that

$$\sum_{j=1}^{d+1} \alpha_j |a_j\rangle \otimes |b_j\rangle = 0 \,. \tag{16}$$

Now let $\{|e_k\rangle\}$ be an orthonormal basis for $\mathcal{H}_B$. Then

$$\sum_{j=1}^{d+1} \alpha_j \langle e_k, b_j\rangle |a_j\rangle = 0 \quad \forall\, k \,. \tag{17}$$

Since the first d vectors $|a_j\rangle$ are linearly independent, there is a vector $\mathbf{x}$ in $\mathbf{C}^{d+1}$ such that $\sum_j v_j |a_j\rangle = 0$ if and only if $\mathbf{v}$ is a multiple of $\mathbf{x}$. Applying this to the coefficients in (17) one finds that there are numbers ν_k such that $u_j \langle e_k, |b_j\rangle = \nu_k x_j$. Let $|\nu\rangle$ be the vector $\sum_k \nu_k |e_k\rangle$. Then $\alpha_j |b_j\rangle = x_j |\nu\rangle$. Since $|b_j\rangle$ was chosen to have norm 1, it follows that when $\alpha_j \neq 0$, $|\frac{x_j}{\alpha_j}| = 1$ and $|b_j\rangle = e^{i\theta_j}|\nu\rangle$. Thus, one can rewrite (15) as

$$\rho = \sum_{j:\alpha_j \neq 0} \lambda_j |a_j\rangle\langle a_j| \otimes |b_j\rangle\langle b_j| + \sum_{j:\alpha_j = 0} \lambda_j |a_j\rangle\langle a_j| \otimes |\nu\rangle\langle \nu| \,. \tag{18}$$

Suppose that t of the α_j are nonzero. Since the vectors $\{a_j\rangle : \alpha_j \neq 0\}$ are linearly dependent, the density matrix $\tilde{\rho}_A = \sum_{j:\alpha_j=0} \lambda_j |a_j\rangle\langle a_j|$ has rank strictly $< t$ and can be rewritten in the form $\tilde{\rho}_A = \sum_{k=1}^{t'} \lambda'_j |a'_j\rangle\langle a'_j|$ using only $t' < t$ vectors. Substituting this in (18) gives ρ as linear combination of products using strictly less than k contradicting the assumption that (15) used the minimum number. □

Proof of (C). If Φ can be written with fewer than d Kraus operators, it is not entanglement breaking; and if it requires more than d Kraus operators, it is not extreme. Hence we can assume that $\mathrm{rank}[(I \otimes \Phi)(|\beta\rangle\langle\beta|) = d$. The result then follows from Lemma 8. □

We now show that, for $d = 3$, the set of entanglement breaking maps has extreme points which are not CQ. Moreover, unlike the $d = 4$ example considered earlier, there is no decomposition into orthogonal blocks associated with this map.

Counterexample. Let $|0\rangle$, $|1\rangle$, $|2\rangle$ be an orthonormal basis for $\mathbf{C}^3$ and consider the following four vectors corresponding to the vertices of a tetrahedron

$$|v_0\rangle = \frac{1}{\sqrt{3}}(+|0\rangle + |1\rangle + |2\rangle)$$

$$|v_1\rangle = \frac{1}{\sqrt{3}}(+|0\rangle - |1\rangle - |2\rangle)$$

$$|v_2\rangle = \frac{1}{\sqrt{3}}(-|0\rangle + |1\rangle - |2\rangle)$$

$$|v_3\rangle = \frac{1}{\sqrt{3}}(-|0\rangle - |1\rangle + |2\rangle)$$

and let

$$\Phi(\rho) = \frac{3}{4}\sum_{i=0}^{3} |v_i\rangle\langle v_i| \,\mathrm{Tr}\,\rho |v_i\rangle\langle v_i| \,. \tag{19}$$

We now show that Φ is an extreme point for the set of entanglement-breaking maps. To see this, first recall that any entanglement breaking map Ψ can be written as

$$\Psi(\rho) = \sum_i \alpha_i |y_i\rangle\langle y_i| \,\mathrm{Tr}\,\rho |z_i\rangle\langle z_i| \,. \tag{20}$$

Let Ψ be one of the entanglement breaking maps whose convex combination is Φ, and let $|y\rangle$ and $|z\rangle$ be $|y_i\rangle$ and $|z_i\rangle$ for some fixed i in this above expression for Ψ. Now, consider the six vectors $|w_{ij}\rangle$ for $i < j$, where these are defined so that $\langle w_{ij}|v_k\rangle = 0$ for $k \neq i, j$. For example, $|w_{01}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$. Then,

$$\Phi(|w_{ij}\rangle\langle w_{ij}|) = \frac{1}{2}(|v_i\rangle\langle v_i| + |v_j\rangle\langle v_j|) \tag{21}$$

so for input $|w_{ij}\rangle\langle w_{ij}|$, the output has rank 2 and is orthogonal to w_{kl}, where i, j, k, l are all distinct. We thus have that for $|y\rangle$ and $|z\rangle$,

$$\langle w_{ij}|y\rangle = 0 \quad \text{or} \quad \langle w_{kl}|z\rangle = 0 \tag{22}$$

where $\{i, j, k, l\}$ is any permutation of $\{0, 1, 2, 3\}$, as above.

Now, consider $|y\rangle$. Suppose it is orthogonal to two of w_{01}, w_{02}, and w_{12}. Then, we must have $|y\rangle = |v_3\rangle$. This means that $|y\rangle$ is not orthogonal to w_{23}, w_{13} and

w_{03}, which implies in turn that $|z\rangle$ is orthogonal to w_{01}, w_{02} and w_{12}, showing that $|z\rangle = |v_3\rangle$ as well.

The other case is when y is not orthogonal to at least two of the above three vectors w_{01}, w_{02}, w_{12}; we can assume by symmetry that these two are w_{01} and w_{02}. Then z is orthogonal to w_{23} and w_{13}, showing that $|z\rangle = |v_0\rangle$. By the same reasoning as in the last paragraph, we now have that $|y\rangle = |v_0\rangle$ as well.

Thus, all the y_i and z_i in the above expression for Ψ must be one of the four vectors v_j. It follows easily from this that $\Psi = \Phi$. Moreover, we have shown that the Holevo form for Φ is essentially unique. Hence Φ cannot be written in the form required for it to be a CQ map.

Note that Φ is not extreme in the set of CPT maps. In fact, it can be represented as a convex combination of CPT maps in several ways. For example, it can be written as the convex combination of the identity map, with weight $\frac{1}{3}$, and the average of the three CP maps that first project the state into one of the three planes $\{|0\rangle, |1\rangle\}$, $\{|0\rangle, |2\rangle\}$, $\{|1\rangle, |2\rangle\}$, and then apply the σ_x operator for that plane interchanging the two basis states, with weight $\frac{2}{3}$. It can also be written as a convex combination of the identity and the four maps corresponding to conjugation with a unitary map which reflects across the plane orthogonal to one of the vectors $|v_j\rangle$.

4. Representations in Bases

Let $G_0 = d^{-1/2} I$ and let $G_1 \cdots G_{d^2-1}$ be a basis for the subspace of self-adjoint $d \times d$ matrices with trace zero which is orthonormal in the sense $\operatorname{Tr} G_j^* G_k = \delta_{jk}$. Then $\{G_k\}$, $k = 0, 1 \cdots d^2 - 1$ is an orthonormal basis for the subspace of self-adjoint $d \times d$ matrices and every density matrix can be written in the form

$$\rho = \frac{1}{d} I + \sum_{j=1}^{d^2-1} w_j G_j = \sum_{j=0}^{d^2-1} w_j G_j \tag{23}$$

with $w_j = \operatorname{Tr} \rho G_j$ so that $w_0 = d^{1/2}$. It then follows that

$$\sum_{j=0}^{d^2-1} w_j^2 = \operatorname{Tr} \rho^2 \leq \operatorname{Tr} \rho = 1 \quad \text{and} \quad \sum_{j=1}^{d^2-1} w_j^2 \leq \frac{d-1}{d}\,.$$

Then any linear (and hence stochastic) map Φ on the self-adjoint $d \times d$ matrices can be represented as a $d^2 \times d^2$ matrix $\mathbf{T}$ with elements $t_{jk} = \operatorname{Tr} G_j \Phi(G_k)$. Now let Φ be a Holevo channel with density matrices $R_k = \sum_j w_j^k G_j$ and POVM $F_k = \sum_n u_n^k G_n$ $(k = 1 \cdots N)$ and write $\rho = \sum_i x_i G_i$. Then it is straightforward to verify that $t_{jn} = \sum_k w_j^k u_n^k$. Thus, $\mathbf{T} = W^T U$ where W and U are the $d^2 \times N$ matrices with elements $w_{jk} = w_j^k$ and $u_{nk} = u_n^k$ respectively. The condition that $\{F_k\}$ is a POVM is precisely that the first row of $\mathbf{T}$ is $(1, 0, \ldots, 0)$.

Such representations have been studied in more detail for qubits using the Pauli matrices for G_k. Recently, several generalizations have been considered for

$d = 3$ [15] and higher [3, 17]. Another natural choice of basis has $G_{jk} = |j\rangle\langle k|$ for some orthonormal basis $|j\rangle$. In this case some modifications are needed since $I = \sum_k G_{kk}$. For $j < k$, one could also replace G_{jk}, G_{kj} by $2^{-1/2}(G_{jk} \pm G_{kj})$ which act like σ_x and $i\sigma_y$ for the two-dimensional subspace span$\{|j\rangle, |k\rangle\}$. Unfortunately, when $d > 2$, the requirement that R_k and F_k are positive semi-definite does not seem easily related to a condition between u_0 and $\sum_{j=1}^{d^2-1} u_j^2$ in any of these bases. Hence, such representations seem most useful for qubits, as discussed in [18].

For a CQ or QC channel, W and U are $d^2 \times d$ which implies rank$(\mathbf{T}) \leq d$. Hence the image of a QC or CQ channel lies in a subspace of dim $\leq d - 1$. This raises the question of whether or not a stochastic map for which the image of the set of density matrices lies in a subspace of sufficiently small dimension is always entanglement breaking. (This is true for qubits for which all planar maps are EBT.)

For a basis in which a necessary condition for positive semi-definiteness is $\sum_{i=1}^{d^2-1} |x_i|^2 \leq x_0^2$, one can show that EBT implies $\sum_{j=1}^{d^2-1} |t_{jj}| \leq 1$. For details, see Ref. 18.

In general, a matrix $\mathbf{T}$ can be written as a product in many ways. We have shown that $\mathbf{T}$ represents an entanglement-breaking map if it can be decomposed into a product $\mathbf{T} = W^T U$ whose elements W, U have very special properties. There is also a correspondence between the matrix $\mathbf{T}$ which represents Φ in a basis in the usual sense and the matrix $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$. It would seem that the requirement that $(I \otimes \Phi)(|\beta\rangle\langle\beta|)$ is separable is related to the product decomposition of $\mathbf{T}$; however, we have not analyzed this. It may be more amenable to the filtering approach advocated by Verstraete and Verschelde [21].

Acknowledgment

Part of this work was done while the authors participated in the program on Quantum Computation at the Mathematical Sciences Research Institute at Berkeley in November, 2002.

The work of M.H. is supported by EC, grant EQUIP (IST-1999-11053), RESQ (IST-2001-37559) and QUPRODIS (IST-2001-38877). The work of M.B.R. was partially supported by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) contract numbers DAAG55-98-1-0374 and DAAD19-02-1-0065, and by the National Science Foundation under Grant number DMS-0074566.

References

[1] C. H. Bennett, D. P. DiVincenzo, J. Smolin and W. K. Wootter, Mixed-state entanglement and quantum error correction, *Phys. Rev. A* **54** (1996), 3824–3851, quant-ph/9604024.

[2] M.-D. Choi, Completely positive linear maps on complex matrices, *Lin. Alg. Appl.* **10** (1975), 285–290.

[3] J. Cortese, The Holevo–Schumacher–Westmoreland channel capacity for a class of qudit unital channels, quant-ph/0211093.

[4] D. P. DiVincenzo, B. M. Terhal and A. V. Thapliyal, Optimal decompositions of barely separable states, *J. Mod. Optics* **47** (2000), 377–385, quant-ph/9904005.
[5] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal and A. V. Thapliyal, Evidence for bound entangled states with negative partial transpose, *Phys. Rev. A* **61**, 062312 (2000), quant-ph/9910026.
[6] A. S. Holevo, Coding theorems for quantum channels, *Russian Math. Surveys* **53** (1999), 1295–1331, quant-ph/9809023.
[7] M. Hordecki, P. Hordecki and R. Hordecki, Separability of mixed states: necessary and sufficient conditions, *Phys. Lett.* **A223** (1996), 1–8.
[8] M. Horodecki and P. Horodecki, Reduction criterion of separability and limits for a class of protocols of entanglement distillation, *Phys. Rev. A* **59** (1999), 4206–4216, quant-ph/9708015.
[9] M. Horodecki, P. Horodecki and R. Horodecki, Binding entanglement channels, *J. Mod. Opt.* **47** (2000), 347–354, quant-ph/9904092.
[10] P. Hordecki, M. Lewenstein, G. Vidal and I. Cirac, Operational criterion and constructive checks for the separability of low rank density matrices, *Phys. Rev. A* **62**, 032310 (2000), quant-ph/0002089.
[11] P. Horodecki, J. Smolin, B. Terhal and A. Thapliyal, Rank two bound entangled states do not exist, *J. Theor. Comp. Sci.* **292** (2003), 589–596, ArXiv.org preprint quant-ph/9910122.
[12] A. Jamiołkowski, Linear transformations which preserve trace and positive semi-definiteness of operators, *Rep. Math. Phys.* **3** (1972), 275–278.
[13] C. King, Maximization of capacityand l_p norms for some product channels, *J. Math. Phys.* **43** (2002), 1247–1260.
[14] C. King, Maximal p-norms of entanglement breaking channels, *Quant. Information and Computation* **3** (2003), 186–190, quant-ph/0212057.
[15] C. King, Capacity of the depolarizing channel, Lecture in workshop on Quantum Information and Cryptography at Mathematical Sciences Research Institute (November, 2002).
http://www.msri.org/publications/ln/msri/2002/quantumcrypto/king/1/index.html
[16] D. Leung, Choi's proof as a recipe for quantum process tomography, *J. Math. Phys.* **44** (2003), 528–533, quant-ph/0201119.
[17] A. O. Pittenger and M. H. Rubin, Separability and Fourier representations of density matrices, *Phys. Rev. A* **62**, 032313 (2000), quant-ph/0001014.
[18] M. B. Ruskai, Qubit entanglement breaking maps, quant-ph/0302032, *Rev. Math. Phys.* **15** (2003), 643–662.
[19] M. B. Ruskai, S. Szarek and W. Werner, An analysis of completely positive trace-preserving maps on $\mathcal{M}_2$, *Lin Alg. Appl.* **347** (2002), 159–187, quant-ph/0101003.
[20] P. W. Shor, Additivity of the classical capacity of entanglement-breaking quantum channels, *J. Math. Phys.* **43** (2002), 4334–4340, quant-ph/0201149.
[21] F. Verstraete and H. S. Verschelde, On one-qubit channels, ArXiv.org preprint quant-ph/0202124, version 1.
[22] G. Vidal, W. Dür and J. I. Cirac, Entanglement cost of bipartite mixed states, *Phys. Rev. Lett.* **89**, 027901 (2002), quant-ph/0112131.