Math. Ann. (2009) 343:757–771
DOI 10.1007/s00208-008-0288-2

Mathematische Annalen

Quantum channels that preserve entanglement

William Arveson

Received: 14 January 2008 / Revised: 18 August 2008 / Published online: 24 September 2008

Abstract Let M and N be full matrix algebras. A unital completely positive (UCP) map $\phi : M \to N$ is said to *preserve entanglement* if its inflation $\phi \otimes \mathrm{id}_N : M \otimes N \to N \otimes N$ has the following property: for every maximally entangled pure state ρ of $N \otimes N$, $\rho \circ (\phi \otimes \mathrm{id}_N)$ is an entangled state of $M \otimes N$. We show that there is a dichotomy in that every UCP map that is not entanglement breaking in the sense of Horodecki–Shor–Ruskai must preserve entanglement, and that entanglement preserving maps of every possible rank exist in abundance. We also show that with probability 1, *all* UCP maps of relatively small rank preserve entanglement, but that this is not so for UCP maps of maximum rank.

Mathematics Subject Classification (2000) Primary: 46N50, Secondary: 81P68 · 94B27

1 Introduction

Let H and K be finite dimensional Hilbert spaces. In the literature of quantum information theory, a *quantum channel* (from $\mathcal{B}(H)$ to $\mathcal{B}(K)$) can be described equivalently as a completely positive linear map

$$\psi : \mathcal{B}(H)' \to \mathcal{B}(K)' \tag{1.1}$$

from the dual of $\mathcal{B}(H)$ to the dual of $\mathcal{B}(K)$ that carries states to states. One can view quantum channels as the morphisms of a category whose objects are the dual spaces $\mathcal{B}(H)'$ of finite dimensional type I factors $\mathcal{B}(H)$. Quantum channels are the *adjoints*

W. Arveson (✉)
Department of Mathematics, University of California, Berkeley, CA, USA
e-mail: arveson@math.berkeley.edu

of unital completely positive (UCP) maps in the sense that the most general map ψ of (1.1) must have the form

$$\psi(\rho) = \rho \circ \phi, \quad \rho \in \mathcal{B}(H)',$$

where $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ is a UCP map. In this paper we focus on UCP maps, keeping in mind that all statements about the category of UCP maps (with objects $\mathcal{B}(H)$) translate contravariantly into statements about the category of quantum channels (with objects $\mathcal{B}(H)'$).

A state ρ of $\mathcal{B}(K \otimes H)$ is called *separable* if it is a convex combination of product states

$$\rho(a \otimes b) = \sum_{k=1}^{s} t_k \cdot \sigma_k(a)\tau_k(b), \quad a \in \mathcal{B}(K), \quad b \in \mathcal{B}(H), \tag{1.2}$$

where σ_k and τ_k are states of $\mathcal{B}(K)$ and $\mathcal{B}(H)$ respectively, and the t_k are positive numbers with sum 1. States that are not separable are said to be *entangled*. Since the set of all separable states of $\mathcal{B}(K \otimes H)$ is compact (see Remark 1.1 of [2]), the entangled states form a relatively open subset of the state space of $\mathcal{B}(K \otimes H)$.

Since the tensor product of two completely positive maps is completely positive, every UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ gives rise to an inflated UCP map $\phi \otimes \mathrm{id} : \mathcal{B}(K \otimes H) \to \mathcal{B}(H \otimes H)$, defined uniquely by sending $a \otimes b$ to $\phi(a) \otimes b$, $a \in \mathcal{B}(K)$, $b \in \mathcal{B}(H)$. In turn, $\phi \otimes \mathrm{id}$ induces a map from states ρ of $\mathcal{B}(H \otimes H)$ to states $\rho' = \rho \circ (\phi \otimes \mathrm{id})$ of $\mathcal{B}(K \otimes H)$:

$$\rho'(a \otimes b) = \rho(\phi(a) \otimes b), \quad a \in \mathcal{B}(K), \quad b \in \mathcal{B}(H). \tag{1.3}$$

The notion of an entanglement breaking channel was introduced and studied in the papers [6,8]. In our context, a UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ is said to be *entanglement breaking* iff for every state ρ of $\mathcal{B}(H \otimes H)$, the state $\rho' = \rho \circ (\phi \otimes \mathrm{id})$ is a separable state of $\mathcal{B}(K \otimes H)$. It was pointed out that entanglement breaking UCP maps are the most degenerate, where in this case "degeneracy" means that the associated quantum channel can be simulated by a classical channel. That is because, as shown in [6], the entanglement breaking UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ are precisely those that admit a representation of the form

$$\phi(x) = \sum_{k=1}^{s} \omega_k(x) e_k, \quad x \in \mathcal{B}(K), \tag{1.4}$$

where $\omega_1, \ldots, \omega_s$ are states of $\mathcal{B}(K)$ and $e_1, \ldots, e_s$ are positive operators in $\mathcal{B}(H)$ having sum $\mathbf{1}$.

We now introduce a class of UCP maps that appear to lie at the opposite extreme from the entanglement breaking ones. Fix a UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ and consider the action of the channel $\phi \otimes \mathrm{id}$ on *pure* states ρ of $\mathcal{B}(H \otimes H)$. If

$x \in \mathcal{B}(H \otimes H) \mapsto \langle x\xi, \xi\rangle$ is the pure state corresponding to a unit vector $\xi \in H \otimes H$, then the corresponding state ρ_ξ of $\mathcal{B}(K \otimes H)$ defined by (1.3) becomes

$$\rho_\xi(a \otimes b) = \langle(\phi(a) \otimes b)\xi, \xi\rangle, \quad a \in \mathcal{B}(K), \quad b \in \mathcal{B}(H). \tag{1.5}$$

Notice that whenever $\xi = \eta \otimes \zeta$ decomposes into a tensor product of vectors in H, ρ_ξ decomposes into a tensor product of states. In order to rule out such "classical" correlations in pure states, we fix attention on unit vectors $\xi \in H \otimes H$ that are *marginally cyclic* in the sense that they satisfy

$$(\mathcal{B}(H) \otimes \mathbf{1})\xi = H \otimes H, \tag{1.6}$$

or equivalently (see Remark 1.2), for every $b \in \mathcal{B}(H)$ one has

$$(\mathbf{1} \otimes b)\xi = 0 \Longrightarrow b = 0.$$

Note that the second assertion is simply that the state of $\mathcal{B}(H)$ defined by $\omega(b) = \langle(\mathbf{1} \otimes b)\xi, \xi\rangle$ should be *faithful*: $\omega(b^*b) = 0 \Longrightarrow b = 0$.

Definition 1.1 A UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ is said to *preserve entanglement* if for every marginally cyclic unit vector $\xi \in H \otimes H$, the state ρ_ξ of (1.5) is an entangled state of $\mathcal{B}(K \otimes H)$.

Remark 1.2 (Relation to maximally entangled pure states) Let H be a finite dimensional Hilbert space. We offer some remarks to support our singling out of marginally cyclic vectors as candidates for "highly entangled" pure states of $\mathcal{B}(H \otimes H)$. There is general agreement in the literature of quantum information theory that the pure states of $\mathcal{B}(H \otimes H)$ that are associated with vectors of the form

$$\xi = n^{-1/2}(e_1 \otimes f_1 + \cdots + e_n \otimes f_n),$$

where (e_k) and (f_k) are orthonormal bases for H, are properly thought of as the "maximally entangled" pure states. These pure states are characterized by the property that their restriction to either subfactor $\mathcal{B}(H) \otimes \mathbf{1}$ or $\mathbf{1} \otimes \mathcal{B}(H)$ should be the tracial state.

One can weaken the latter requirement on a pure state ρ of $\mathcal{B}(H \otimes H)$

$$\rho(x) = \langle x\xi, \xi\rangle, \quad x \in \mathcal{B}(H \otimes H)$$

by requiring that its "marginal" state ω, defined on $\mathcal{B}(H)$ by

$$\omega(b) = \langle(\mathbf{1} \otimes b)\xi, \xi\rangle, \quad b \in \mathcal{B}(H),$$

should have a density operator of maximum rank; or equivalently, that ω should *faithful* in the sense that

$$\omega(b^*b) = 0 \Longrightarrow b = 0, \quad b \in \mathcal{B}(H).$$

The latter property is equivalent to the assertion that for every $b \in \mathcal{B}(H)$,

$$(\mathbf{1} \otimes b)\xi = 0 \Longrightarrow b = 0. \tag{1.7}$$

In turn, since the two von Neumann algebras $\mathcal{B}(H) \otimes \mathbf{1}$ and $\mathbf{1} \otimes \mathcal{B}(H)$ are commutants of each other, (1.7) is equivalent to the assertion of (1.6), namely that ξ should be a marginally cyclic vector. For this reason, we have found it useful to regard a unit vector $\xi \in H \otimes H$ as "highly entangled" (but perhaps not maximally entangled) precisely when it is marginally cyclic.

In Sect. 2 we show how the parameterization of states given in [2] can be appropriately adapted to UCP maps so as to make the space Φ^r of all UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ of rank $\leq r$ into a compact probability space that carries a unique unbiased probability measure P^r, and we show in Sect. 4 that P^r is concentrated on the set of maps of rank r. Thus, the probability space (Φ^r, P^r) represents *choosing a UCP map of rank r at random*. We prove a zero-one law for channels in Sect. 3 which expresses in strong probabilistic terms the dichotomy that a UCP map either preserves entanglement or it has the degenerate form (1.4).

We then apply the main results of [2] to show that there are plenty of entanglement preserving UCP maps of every possible rank, and that *almost surely every* UCP map of relatively small rank preserves entanglement (see Theorem 4.2). We conclude with a discussion of extreme points of the convex set of UCP maps that implies: Whenever an extremal UCP map of rank r exists, then almost surely every UCP map of rank r is extremal.

Since writing this paper, we learned from M. B. Ruskai that a definition of "maximally entangled pure state" has been proposed in [3,5] that is equivalent to the above definition of marginally cyclic vector (such vectors are said to have "maximum Schmidt rank" in [3,5]). Basically, those authors obtain information about the relations between subspaces $M \subseteq H \otimes H$ with the property that every unit vector in M has "Schmidt rank" at least r and they apply their results to some of the measures of entanglement that have been proposed in the literature of quantum information theory.

2 Real-analytic parameters for UCP maps

Let H and K be finite dimensional Hilbert spaces with $n = \dim H$, $m = \dim K$ and fix a UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$. A straightforward application of Stinespring's theorem (as formulated in Appendix A) implies that there is an r-tuple of operators $v_1, \dots, v_r \in \mathcal{B}(H, K)$ such that

$$\phi(a) = v_1^* a v_1 + \cdots + v_r^* a v_r, \quad a \in \mathcal{B}(K), \tag{2.1}$$

and that the operators v_k satisfy

$$v_1^* v_1 + \cdots + v_r^* v_r = \mathbf{1}_H. \tag{2.2}$$

Moreover, one can arrange that $v_1, \dots, v_r$ are linearly independent, and in that case the integer r is called the *rank* of ϕ. Let $\Phi^r(K, H)$ be the compact space of all UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ of rank at most r. Since H and K will be held fixed, we lighten notation by writing Φ^r for $\Phi^r(K, H)$.

In this section we show that for every $r = 1, 2, \dots, mn$, there is a convenient parameterization of the space Φ^r and we describe its basic properties. While this is a reformulation of some of the results of [2], there are enough differences in the two formulations that it is appropriate to discuss this parameterization of Φ^r in some detail.

Given two r-tuples $(v_1, \dots, v_r)$ and $(v'_1, \dots, v'_r)$ of operators in $\mathcal{B}(H, K)$ which are *not* necessarily linearly independent, then by Proposition A.1 of Appendix A,

$$v_1^* x v_1 + \cdots + v_r^* x v_r = v_1'^* x v_1' + \cdots + v_r'^* x v_r', \quad x \in \mathcal{B}(K)$$

iff there is a unitary $r \times r$ matrix $(\lambda_{ij}) \in M_r(\mathbb{C})$ such that

$$v'_i = \sum_{j=1}^{r} \lambda_{ij} v_j, \quad i = 1, 2, \dots, r. \tag{2.3}$$

Now consider the space $V^r(H, K)$ of all r-tuples $v = (v_1, \dots, v_r)$ with operator components $v_k \in \mathcal{B}(H, K)$ that satisfy $v_1^* v_1 + \cdots + v_r^* v_r = \mathbf{1}_H$ (we do *not* require that the component operators are linearly independent). Theorem 2.1 of [2] implies that $V^r(H, K)$ is a compact connected real-analytic Riemannian manifold that is acted upon transitively by a compact group of isometries. For every $v = (v_1, \dots, v_r) \in V^r(H, K)$,

$$\phi_v(x) = v_1^* x v_1 + \cdots + v_r^* x v_r, \quad x \in \mathcal{B}(K) \tag{2.4}$$

defines a UCP map $\phi_v : \mathcal{B}(K) \to \mathcal{B}(H)$ of rank at most r. The following result summarizes the properties of this parameterization $v \mapsto \phi_v$ and is a direct consequence of the preceding remarks. We write $U(r)$ for the group of all unitary $r \times r$ matrices.

Proposition 2.1 *Fix two finite dimensional Hilbert spaces H, K with* $\dim H = n$, $\dim K = m$. *For every $r = 1, 2, \dots, mn$, let Φ^r be the compact space of all UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ of rank $\le r$.*

Every element of Φ^r has the form (2.4) for some $v \in V^r(H, K)$. This parameterization $v \mapsto \phi_v$ is continuous and one has $\phi_v = \phi_{v'}$ iff v and v' belong to the same $U(r)$ orbit as in (2.3). Hence the map $v \mapsto \phi_v$ promotes uniquely to a homeomorphism of the orbit space $V^r(H, K)/U(r)$ onto the space Φ^r of UCP maps of rank $\le r$.

Fixing H, K as in Proposition 2.1, consider the integer $q = m^2n^2 + 1$, and the much larger unitary group $U(q)$. We single out the following subset of $V^r(H, K)$,

$$\mathrm{Sep}(V^r(H, K)) = \bigcup_{\lambda \in U(q)} Z_\lambda,$$

where

$$Z_\lambda = \{w = (w_1, \dots, w_r) \in V^r(H, K) : \operatorname{rank}(\sum_{j=1}^{r} \lambda_{ij} w_j) \le 1, \quad 1 \le i \le q\}.$$

The key property of $\operatorname{Sep}(V^r(H, K))$ is described as follows.

Proposition 2.2 *Let $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ be a UCP map of rank r, choose $v \in V^r(H, K)$ so that $\phi = \phi_v$, and let $\xi \in H \otimes H$ be a marginally cyclic unit vector. Then the state ρ_ξ of $\mathcal{B}(K \otimes H)$ defined by*

$$\rho_\xi(a \otimes b) = \langle(\phi_v(a) \otimes b)\xi, \xi\rangle, \quad a \in \mathcal{B}(K), \quad b \in \mathcal{B}(H)$$

is separable iff $v \in \operatorname{Sep}(V^r(H, K))$.

Proof This is a restatement of Proposition 7.7 of [2]. □

After noting that the condition $v \in \operatorname{Sep}(V^r(H, K))$ does not depend on the choice of marginally cyclic vector ξ, we can combine Proposition 2.2 with a result of [6] to conclude:

Corollary 2.3 *Let $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ be an arbitrary UCP map and let $\mathcal{S}_\phi$ be the set of all states ρ of $\mathcal{B}(K \otimes H)$ of the form*

$$\rho(a \otimes b) = \langle(\phi(a) \otimes b)\xi, \xi\rangle, \quad a \in \mathcal{B}(K), \quad b \in \mathcal{B}(H), \tag{2.5}$$

where ξ ranges over the set of marginally cyclic unit vectors in $H \otimes H$. If $\mathcal{S}_\phi$ contains a single entangled state then every state of $\mathcal{S}_\phi$ is entangled and ϕ preserves entanglement. Otherwise, ϕ is entanglement breaking.

Proof To prove the last sentence, let $e_1, \dots, e_n$ be an orthonormal basis for H and let ξ be the marginally cyclic unit vector

$$\xi = \frac{1}{\sqrt{n}}(e_1 \otimes e_1 + \cdots + e_n \otimes e_n).$$

The implications B $\iff$ C of Theorem 4 of [6] are equivalent to the assertion that ϕ is entanglement breaking iff the state ρ is separable, hence the assertion follows from the first two sentences of Corollary 2.3. □

3 A zero-one law for UCP maps

The unit sphere $S(H) = \{\xi \in H : \|\xi\| = 1\}$ of an n dimensional Hilbert space H is S^{2n-1}, a real-analytic Riemannian symmetric space that carries a unique unitarily invariant probability measure μ_H.

Fix a UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$. Every vector ξ in the unit sphere of $H \otimes H$ gives rise to a state ρ_ξ of $\mathcal{B}(K \otimes H)$ by way of

$$\rho_\xi(a \otimes b) = \langle (\phi(a) \otimes b)\xi, \xi \rangle, \quad a \in \mathcal{B}(K), \quad b \in \mathcal{B}(H), \tag{3.1}$$

thereby obtaining a map $\hat{\phi} : \xi \mapsto \rho_\xi$ from $S(H \otimes H)$ to states of $\mathcal{B}(K \otimes H)$ that we can view as a random variable associated with the probability space $(S(H \otimes H), \mu_{H \otimes H})$. We now show that it is possible to determine whether ϕ preserves entanglement in a way that makes no reference to marginally cyclic vectors, but rather to properties of the random variable $\hat{\phi}$. Indeed, Theorem 3.1 frames the dichotomy of UCP maps as follows: *The channel associated with an arbitrary UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ either maps all pure states to separable states, or it maps almost all pure states to entangled states.* Perhaps that assertion is expressed more concisely as a zero-one law:

$$\mu_{H \otimes H}\{\xi \in S(H \otimes H) : \hat{\phi}(\xi) \text{ is entangled}\} = 0 \text{ or } 1.$$

Theorem 3.1 *For every UCP map $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$, the following are equivalent:*

(i) *For almost every vector $\xi \in S(H \otimes H)$, the state ρ_ξ is entangled.*
(ii) *For every vector ξ in some Borel subset of $S(H \otimes H)$ of positive measure, the state ρ_ξ of (3.1) is entangled.*
(iii) *ϕ preserves entanglement.*

The proof of Theorem 3.1 requires:

Lemma 3.2 *The set of marginally cyclic unit vectors of $H \otimes H$ is relatively open and dense in $S(H \otimes H)$ and its complement has measure zero.*

Proof Let Z be the set of all vectors $\xi \in S(H \otimes H)$ that are *not* marginally cyclic. Since $\mu_{H \otimes H}$ assigns positive mass to nonempty open subsets of the unit sphere, it suffices to show that Z is a closed set of $\mu_{H \otimes H}$-measure zero. Since the unit sphere $S(H \otimes H)$ is a connected real-analytic submanifold of its ambient space $H \otimes H$, for every real-analytic function

$$F : S(H \otimes H) \to W \tag{3.2}$$

that takes values in a finite dimensional real vector space W, either F vanishes identically or the set of zeros of F is a closed set of $\mu_{H \otimes H}$-measure zero (see Proposition B.1 of [2]). Thus, in order to show that $\mu_{H \otimes H}(Z) = 0$, it suffices to exhibit a real-analytic function F as in (3.2) that does not vanish identically on $S(H \otimes H)$ such that $Z = \{\xi \in S(H \otimes H) : F(\xi) = 0\}$.

We exhibit such a function F as follows. We view $H \otimes H$ as $\mathbb{C}^n \otimes H$, where $n = \dim H$, in which case $\mathbb{C}^n \otimes H$ is identified with the direct sum of n copies of H, $\mathbf{1}_{\mathbb{C}^n} \otimes \mathcal{B}(H)$ is identified with $n \times n$ diagonal operator matrices (b_{ij}) with $b_{11} = \cdots = b_{nn} \in \mathcal{B}(H)$, and its commutant $\mathcal{B}(\mathbb{C}^n) \otimes \mathbf{1}_H$ is identified with the set of all $n \times n$ operator matrices with entries in $\mathbb{C} \cdot \mathbf{1}_H$.

Let $\xi = (\xi_1, \dots, \xi_n)$ be a unit vector in $\mathbb{C}^n \otimes H$. Viewing ξ as a column vector, straightforward verification shows that ξ is marginally cyclic, i.e., $(\mathcal{B}(\mathbb{C}^n) \otimes \mathbf{1})\xi = \mathbb{C}^n \otimes H$, iff its components satisfy

$$\operatorname{span}\{\xi_1, \dots, \xi_n\} = H,$$

or equivalently, iff $\{\xi_1, \dots, \xi_n\}$ is linearly independent.

Consider the function $F : \mathbb{C}^n \otimes H \to \wedge^n H = H \wedge \cdots \wedge H$ defined by

$$F(\xi_1, \dots, \xi_n) = \xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n.$$

F is a homogeneous polynomial of degree n, and elementary multilinear algebra shows that for every $(\xi_1, \dots, \xi_n) \in \mathbb{C}^n \otimes H$, the components ξ_k form a linearly independent set iff $\xi_1 \wedge \cdots \wedge \xi_n \neq 0$. Hence the restriction of F to the unit sphere $S(\mathbb{C}^n \otimes H)$ is a real-analytic function with the property $Z = \{\bar{\xi} \in S(\mathbb{C}^n \otimes H) : F(\bar{\xi}) = 0\}$. Obviously, F does not vanish identically on $S(\mathbb{C}^n \otimes H)$, since it is nonzero on any n-tuple $\bar{\xi} = (\xi_1, \dots, \xi_n)$ with linearly independent components ξ_k. □

Proof of Theorem 3.1 (i) $\Longrightarrow$ (ii) is trivial.

(ii) $\Longrightarrow$ (iii): Let E be a Borel subset of $S(H \otimes H)$ of positive measure such that ρ_ξ is entangled for every $\xi \in E$. By Lemma 3.2, the set M of marginally cyclic vectors in $S(H \otimes H)$ is an open dense set whose complement has measure zero. Hence $M \cap E$ must have positive measure, and is therefore nonempty. Every element of $M \cap E$ is a marginally cyclic unit vector ξ for which ρ_ξ is entangled, and at this point (iii) follows from Corollary 2.3.

(iii) $\Longrightarrow$ (i): This is immediate from Corollary 2.3 and Lemma 3.2. □

4 Abundance of entanglement preserving maps

Throughout this section, H and K denote Hilbert spaces of respective finite dimensions n and m, and for the main results below we require that $n \leq m$. Proposition 2.1 asserts that for every $r = 1, 2, \dots, mn$, the map

$$v \in V^r(H, K) \mapsto \phi_v \in \Phi^r$$

promotes to a homeomorphism of the orbit space $V^r(H, K)/U(r)$ onto the compact space Φ^r of all UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ of rank $\leq r$. The unique invariant probability measure μ of $V^r(H, K)$ promotes to a probability measure P^r on Φ^r, defined on Borel sets $E \subseteq \Phi^r$ by

$$P^r(E) = \mu\{v \in V^r(H, K) : \phi_v \in E\},$$

and Theorem 3.3 of [2] is equivalent to the following key assertion about this nonatomic topological probability space (Φ^r, P^r):

Theorem 4.1 *For each $r = 1, \dots, mn$, the measure P^r is concentrated on the relatively open subset of Φ^r consisting of UCP maps of rank $= r$.*

We conclude that *for every* $r = 1, 2, \ldots, mn$, *the probability space* (Φ^r, P^r) *represents "choosing a UCP map of rank r at random"*.

In the following result we convert the principal results of [2] into assertions about the probability space (Φ^r, P^r). We write $EP(\Phi^r)$ for the set of all entanglement preserving maps in Φ^r.

Theorem 4.2 *Let* H, K *satisfy* $n = \dim H \leq m = \dim K < \infty$.

(i) *For every* $r = 1, 2, \ldots, mn$, $EP(\Phi^r)$ *is a relatively open subset of* Φ^r *of positive measure.*
(ii) *For every r satisfying* $1 \leq r \leq n/2$, $P^r(EP(\Phi^r)) = 1$.
(iii) *For the maximum rank* $r = mn$ *one has* $0 < P^{mn}(EP(\Phi^{mn})) < 1$.

The proof requires some material from [2], which we summarize for the reader's convenience.

Remark 4.3 (Subvarieties of $V^r(H, K)$) By a *subvariety* of $V^r(H, K)$ we mean a subset of the form $Z = \{v \in V^r(H, K) : F(v) = 0\}$, where

$$F : V^r(H, K) \to W$$

is a real-analytic function taking values in a finite dimensional real vector space W. Let μ be the unique probability measure on $V^r(H, K)$ that is invariant under the transitive action by isometries. Proposition 2.6 of [2] asserts that *every proper subvariety* $Z \neq V^r(H, K)$ *has* μ*-measure zero.*

Remark 4.4 (The wedge invariant) In [2] we introduced an invariant of states called the wedge invariant. The wedge invariant can be interpreted as a pair of random variables on the probability space $(V^r(H, K), \mu)$ as follows. Every r-tuple $v = (v_1, \ldots, v_r) \in V^r(H, K)$ gives rise to an operator $v_1 \wedge \cdots \wedge v_r$ from $\otimes^r H$ to $\otimes^r K$ as in (1.5) of [2], and $v_1 \wedge \cdots \wedge v_r$ maps the symmetric subspace $\otimes^r H_+$ of $\otimes^r H$ to the antisymmetric subspace $\wedge^r K$ of $\otimes^r K$. Similarly, $v_1^* \wedge \cdots \wedge v_r^*$ maps the symmetric subspace of $\otimes^r K$ to the antisymmetric subspace of $\otimes^r H$. Thus we obtain a pair of integer-valued random variables $w(\cdot)$, $w^*(\cdot)$ defined on $V^r(H, K)$ by

$$w(v) = \operatorname{rank}(v_1 \wedge \cdots \wedge v_r \restriction_{\otimes^r H_+}), \quad w^*(v) = \operatorname{rank}(v_1^* \wedge \cdots \wedge v_r^* \restriction_{\otimes^r K_+}).$$

These functions $w(\cdot)$ and $w^*(\cdot)$ are associated with subvarieties as follows. Propositions 8.1 and 8.2 of [2] imply that for every $r = 1, \ldots, mn$,

$$A = \{v \in V^r(H, K) : w(v) \leq 1\}, \quad A^* = \{v \in V^r(H, K) : w^*(v) \leq 1\}$$

are subvarieties of $V^r(H, K)$ and that $\mathrm{Sep}(V^r(H, K)) \subseteq A \cap A^*$.

Proof of Theorem 4.2 (i): Combining the discussion preceding Theorem 4.2 with the discussion of Sect. 2, one sees that the parameterization map $v \mapsto \phi_v$ gives rise to a measure preserving surjection of topological probability spaces $(V^r(H, K), \mu) \to (\Phi^r, P^r)$, which carries the closed set $\mathrm{Sep}(V^r(H, K))$ to the space of entanglement breaking maps of Φ^r and carries its complement to $EP(\Phi^r)$. Hence the assertion (i) is that for every r one has $\mu(\mathrm{Sep}(V^r(H,K)) < 1$, which follows from Theorem 7.8 of [2].

(ii): We have seen that $EP(V^r(H,K)) = V^r(H,K)\setminus \mathrm{Sep}(V^r(H,K))$ is an open set. We make use of the random variable of Remark 4.4

$$w^* : V^r(H,K) \to \mathbb{Z}_+$$

as follows. By Remark 4.4 above, $\mathrm{Sep}(V^r(H,K)) \subseteq A^*$ and A^* is a subvariety of $V^r(H,K)$. The critical fact is that since r does not exceed $n/2$, Proposition 8.3 of [2] implies that A^* is a *proper* subvariety of $V^r(H,K)$, and therefore has μ-measure zero. Hence $\mu(\mathrm{Sep}(V^r(H,K)) = 0$.

(iii): The remark following Proposition 2.2 makes it clear that Theorem 10.1 of [2] is equivalent to the assertion that $EP(\Phi^{mn})$ is a relatively open subset of Φ^r for which $0 < P^r(EP(\Phi^r)) < 1$. □

Remark 4.5 (Estimating the critical rank) Item (i) of Theorem 4.2 asserts that there are plenty of entanglement preserving UCP maps of every possible rank. (ii) asserts that essentially *all* UCP maps of relatively small rank must preserve entanglement, while (iii) implies that this breaks down for maps of maximum rank. Hence there is a critical rank $r_0 \le mn$ with the property that essentially all UCP maps of rank $< r_0$ preserve entanglement, while $0 < P^{r_0}(EP(\Phi^{r_0})) < 1$. As we have pointed out in the context of states in Remark 12.3 of [2], both bounds $n/2 < r_0 \le mn$ that follow directly from Theorem 4.2 seem overly conservative, and one would hope to have considerably more information about the size of r_0 in the future.

5 Abundance of extremals

In this section we continue in the context of UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ where $n = \dim H \le \dim K = m < \infty$. In [9], it was shown (in its dual form) that the extremal UCP maps $\phi : \mathcal{B}(H) \to \mathcal{B}(H)$ are dense in the set of all UCP maps of rank at most n, generalizing a result of [7] for 2×2 matrix algebras. Our final result makes essentially the following assertion about extreme points of the convex set of UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$: *If there is an extremal UCP map of rank r, then almost surely every UCP map of rank r is extremal.*

Theorem 5.1 *For every integer r satisfying $1 \le r \le n$, the extremals of rank r in (Φ^r, P^r) are a relatively open dense set having probability 1. There are no extremal UCP maps $\phi : \mathcal{B}(K) \to \mathcal{B}(H)$ of rank $> n$.*

The proof of Theorem 5.1 requires

Lemma 5.2 *Let r be an integer satisfying $1 \le r \le n \le m$. Then there is an r-tuple $v = (v_1, \dots, v_r) \in V^r(H,K)$ such that $\{v_i^* v_j : 1 \le i, j \le r\}$ is a linearly independent subset of $\mathcal{B}(H)$.*

Proof Let $e_1, \ldots, e_r$ be an orthonormal set in H, let p be the projection onto the linear span of $e_1, \ldots, e_r$ and let f be a unit vector in K. For each $i = 1, \ldots, r$ let u_i be the rank-one partial isometry $u_i\xi = \langle \xi, e_i \rangle f$. Note that $\{u_i^* u_j : 1 \le i, j \le r\}$ defines a system of matrix units for which $u_1^* u_1 + \cdots + u_r^* u_r = p$, and in particular, $\{u_i^* u_j : 1 \le i, j \le r\}$ is a linearly independent subset of $\mathcal{B}(H)$.

The rank of $p^\perp$ is $n - r \le n - 1 \le m - 1$, hence there is a projection $q \in \mathcal{B}(K)$ with $\operatorname{rank} q = \operatorname{rank} p^\perp$ whose range is orthogonal to f. Let w be a partial isometry in $\mathcal{B}(H, K)$ having initial projection $p^\perp$ and final projection q, and set

$$v_i = u_i + r^{-1/2} w, \quad i = 1, 2, \ldots, r.$$

One finds that $v_i^* v_j = u_i^* u_j + r^{-1} p^\perp$, hence $v_1^* v_1 + \cdots + v_r^* v_r = \mathbf{1}_H$, and the set of all $v_i^* v_j = u_i^* u_j \oplus r^{-1} p^\perp$ is obviously linearly independent. □

Remark 5.3 Note that for any set of operators $v_1, \ldots, v_r \in \mathcal{B}(H, K)$ for which $\{v_i^* v_j : 1 \le i, j \le r\}$ is linearly independent, $\{v_1, \ldots, v_r\}$ must be linearly independent. For if $\lambda_i \in \mathbb{C}$ such that $\lambda_1 \cdot v_1 + \cdots + \lambda_r \cdot v_r = 0$, then $\sum_{ij} \bar{\lambda}_i \lambda_j \cdot v_i^* v_j = 0$, hence $\bar{\lambda}_i \lambda_j = 0$ for all i, j, hence $|\lambda_i|^2 = 0$ for all i.

Proof of Theorem 5.1 Consider the complex vector space

$$W = \wedge^{r^2} \mathcal{B}(H) = \mathcal{B}(H) \wedge \cdots \wedge \mathcal{B}(H),$$

the exterior product of r^2 copies of $\mathcal{B}(H)$, and let $F : V^r(H, K) \to W$ be the function obtained by restricting the function

$$v = (v_1, \ldots, v_r) \in \mathcal{B}(H, K)^r \mapsto \bigwedge_{1 \le i, j \le r} v_i^* v_j \in W$$

to $V^r(H, K)$. Since the above function is a real-homogeneous polynomial of degree $2r$, its restriction to $V^r(H, K)$ is real-analytic. Moreover, Lemma 5.2 implies that there is a point $v \in V^r(H, K)$ for which $F(v) \ne 0$. It follows that the set $Z = \{v \in V^r(H, K) : F(v) = 0\}$ of zeros of F is a *proper* subvariety and therefore has measure zero and empty interior (see Remark 4.3). By Remark 5.3 and the remarks following (B.2), for every $v \in V^r(H, K)$, the associated UCP map ϕ_v is extremal of rank r iff $v \notin Z$. This proves that the set of extremals of rank r in Φ^r is an open dense subset whose complement has measure zero.

The second sentence follows from the fact that if $\phi(x) = v_1^* x v_1 + \cdots + v_r^* x v_r$ is extremal of rank r, then by the remarks following (B.2), the set of r^2 operators $\{v_i^* v_j : 1 \le i, j \le r\}$ in $\mathcal{B}(H)$ is linearly independent. Since $\dim \mathcal{B}(H) = n^2$, it follows that $r^2 \le n^2$, hence $r \le n$. □

Appendix A: Remarks on Stinespring's theorem

Stinespring's theorem (Theorem 1 of [10]) provides a familiar and useful representation of completely positive maps. Along with the existence of this representation there are notions of *minimality* and *uniqueness*—both of which have significant consequences, though neither minimality nor uniqueness was mentioned in the original source [10]. We briefly review these facts here since we shall have to make use of all of them in this paper, referring the reader to pp. 143–146 of [1] for more detail.

Let A be a unital C^*-algebra and let $\phi : A \to \mathcal{B}(H)$ be an operator-valued completely positive linear map. The principal assertion of Stinespring's theorem is that there is a pair (π, V) consisting of a representation π of A on another Hilbert space K and an operator $V : H \to K$ such that

$$\phi(x) = V^*\pi(x)V, \quad x \in A. \tag{A.1}$$

Such a pair (π, V) will be called a *Stinespring pair* for ϕ. Two Stinespring pairs (π_1, V_1) and (π_1, V_2) are said to be *equivalent* if there is a unitary operator $U : K_1 \to K_2$ such that

$$UV_1 = V_2, \quad \text{and} \quad U\pi_1(x) = \pi_2(x)U, \quad x \in A. \tag{A.2}$$

A Stinespring pair (π, V) is said to be *minimal* if VH is a cyclic subspace for the representation π in the sense that

$$K = \overline{\text{span}}\,\{\pi(x)V\xi : x \in A, \xi \in H\}. \tag{A.3}$$

The requirement (A.3) is equivalent to the following assertion about the relation of the subspace VH to the commutant $\pi(A)'$:

$$\forall\ b \in \pi(A)', \quad b\restriction_{VH} = 0 \Longrightarrow b = 0. \tag{A.4}$$

Every Stinespring pair (π, V) can be reduced to a minimal one by replacing π with the subrepresentation obtained by restricting π to the reducing subspace of K defined by the right side of (A.3). The uniqueness assertion is simply that *any two minimal Stinespring pairs for ϕ are equivalent.*

The immediate consequences of these results for UCP maps $\phi : \mathcal{B}(H_1) \to \mathcal{B}(H_2)$ between finite dimensional type I factors are as follows. Taking $A = \mathcal{B}(H_1)$ and noting that the most general finite dimensional representation of $\mathcal{B}(H_1)$ is unitarily equivalent to a direct sum of $r = 1, 2, \dots$ copies of the identity representation, we conclude that there is a minimal Stinespring pair of the form (π, V) where π is the representation on $r \cdot H_1$ defined by

$$\pi(x) = \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & x \end{pmatrix}, \quad x \in \mathcal{B}(H_1) \tag{A.5}$$

and where $V : H_2 \to r \cdot H_1 = H_1 \oplus \cdots \oplus H_1$ is a linear map from H_2 to a direct sum of r copies of H_1. The operator $V : H_2 \to r \cdot H_1$ must have the form

$V\xi = (v_1\xi, \dots, v_r\xi)$, $\xi \in H_2$ (viewed as a column vector), where $v_1, \dots, v_r$ is a uniquely determined r-tuple of operators in $\mathcal{B}(H_2, H_1)$. After these adjustments, the formula $\phi(x) = V^*\pi(x)V$ becomes

$$\phi(x) = v_1^* x v_1 + \cdots + v_r^* x v_r, \quad x \in \mathcal{B}(H_1). \tag{A.6}$$

Since the commutant of $\pi(\mathcal{B}(H_1))$ consists of all $r \times r$ operator matrices with entries in $\mathbb{C} \cdot \mathbf{1}_{H_1}$, the equivalence of (A.3) and (A.4) implies that the minimality of (π, V) becomes this assertion: For every $\lambda_1, \dots, \lambda_r \in \mathbb{C}$

$$\lambda_1 v_1 + \cdots + \lambda_r \cdot v_r = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_r = 0,$$

i.e., iff the set of operators $\{v_1, \dots, v_r\}$ that implements (A.6) should be *linearly independent*. In particular, these remarks show that the integer r is uniquely defined by the formula (A.6) when $v_1, \dots, v_r$ is linearly independent; r is called the *rank* of the completely positive map $\phi : \mathcal{B}(H_1) \to \mathcal{B}(H_2)$.

The r-tuple $(v_1, \dots, v_r)$ that implements (A.6) is certainly not unique; but if $(v_1', \dots, v_r')$ is another such r-tuple, then the operator $V' : H_2 \to r \cdot H_1$ defined by

$$V'\xi = (v_1'\xi, \dots, v_r'\xi), \quad \xi \in H_2$$

defines another Stinespring pair (π, V') associated with the same representation of (A.5). After recalling the structure of the commutant of $\pi(\mathcal{B}(H_1))$, one can apply the uniqueness assertion of Stinespring's theorem to conclude that there is a unique unitary matrix of scalars $(\lambda_{ij}) \in U(r)$ such that

$$v_i' = \sum_{j=1}^{r} \lambda_{ij} \cdot v_j, \quad i = 1, 2, \dots, r. \tag{A.7}$$

We require the following somewhat stronger form of uniqueness—known as the Choi–Kraus representation in the physics literature—in which the hypothesis of linear independence is dropped. Notice however that *its proof is fundamentally the same as the proof of the preceding uniqueness assertion.* Note too the resemblance between this result and Proposition 5.1 of [2], which characterizes the possible representations of finite sums of positive rank one Hilbert space operators. Indeed, though we do not require the fact, there is a common generalization of both assertions to Hilbert C^*-modules.

Proposition A.1 *Let $(v_1, \dots, v_r)$ and $(v_1', \dots, v_r')$ be two r-tuples of operators in $\mathcal{B}(H_2, H_1)$. Then one has*

$$v_1^* x v_1 + \cdots + v_r^* x v_r = v_1'^* x v_1' + \cdots + v_r'^* x v_r' \tag{A.8}$$

for all $x \in \mathcal{B}(H_1)$ iff there is a unitary $r \times r$ matrix $(\lambda_{ij}) \in U(r)$ that relates $(v_1', \dots, v_r')$ to $(v_1, \dots, v_r)$ as in (A.7).

Proof Assuming that (A.8) is satisfied, one can set x equal to the identity operator and argue as in the proof of Proposition 5.1 of [2] to obtain the desired unitary matrix (λ_{ij}). The converse is left for the reader. □

Appendix B: Remarks on extremal UCP maps

Let A be a unital C^*-algebra. The extremal UCP maps from A to $\mathcal{B}(H)$ were first determined in Theorem 1.4.6 of [1], which makes the following assertion in that case.

Theorem B.1 *For every UCP map $\phi : A \to \mathcal{B}(H)$, the following are equivalent.*

(i) *ϕ is an extreme point of the convex set of all UCP maps from A to $\mathcal{B}(H)$.*
(ii) *Let (π, V) be a minimal Stinespring pair for ϕ. Then for every operator b in the commutant of $\pi(A)$,*

$$V^*bV = 0 \Longrightarrow b = 0. \tag{B.1}$$

Notice that in general, the condition (B.1) is *stronger* than the condition (A.4) for minimality. Now specialize to the case in which H_1 and H_2 are finite dimensional Hilbert spaces and $\phi : \mathcal{B}(H_1) \to \mathcal{B}(H_2)$ is a UCP map. Choosing an r-tuple of operators $v_1, \dots, v_r \in \mathcal{B}(H_2, H_1)$ as in (A.6)

$$\phi(x) = v_1^* x v_1 + \cdots + v_r^* x v_r, \quad x \in \mathcal{B}(H_1)$$

and letting π be the representation of $\mathcal{B}(H_1)$ on $r \cdot H_1$ defined in (A.5), we obtain a Stinespring pair (π, V) for ϕ by defining $V : H_2 \to r \cdot H_1$ as in Appendix A, viewing $V\xi = (v_1\xi, \dots, v_r\xi)$ for $\xi \in H_2$ as a column vector with components in H_1. Noting the structure of the commutant of $\pi(\mathcal{B}(H_1))$ pointed out in Appendix A following (A.6), one finds that the condition (B.1) for extremality becomes this: for every $r \times r$ matrix of scalars (λ_{ij})

$$\sum_{i,j=1}^{r} \lambda_{ij} \cdot v_i^* v_j = 0 \Longrightarrow \lambda_{ij} = 0, 1 \le i, j \le r, \tag{B.2}$$

and from Theorem B.1 we conclude that ϕ *is extremal iff the set of operators* $\{v_i^* v_j : 1 \le i, j \le r\}$ *is linearly independent*. The latter result is known as Choi's theorem in the quantum information theory literature, which cites [4] as the source.

Acknowledgments I thank Mary Beth Ruskai for helpful remarks concerning material in [6] and for pointing out several references.

References

1. Arveson, W.: Subalgebras of C^*-algebras. Acta Math. **123**, 141–224 (1969)
2. Arveson, W.: The probability of entanglement, pp. 1–31 (2007, preprint) arXiv:0712.4163

3. Cubitt, T., Harrow, A.W., Leung, D., Montanaro, A., Winter, A.: Counterexamples to additivity of minimum output p-Renyi entropy for p close to 0, pp. 1–7 (2007, preprint) arXiv:0712.3628v2
4. Choi, M.-D.: Completely positive maps on complex matrices. Lin. Alg. Appl. **10**, 285–290 (1975)
5. Cubitt, T., Montanaro, A., Winter, A. (2007) On the dimension of subspaces with bounded Schmidt rank, pp. 1–4 (2007, preprint) arXiv:0706.0705v1
6. Horodecki, R., Shor, P., Ruskai, M.B.: Entanglement breaking channels. Rev. Math. Phys. **15**(6), 629–641 (2003) arXiv:quant-ph/0302031
7. Ruskai, M.B., Szarek, S., Werner, E.: An analysis of completely positive trace-preserving maps on M_2. Lin. Alg. Appl. **347**, 159–187 (2002)
8. Ruskai, M.B.: Qubit entanglement breaking channels. Rev. Math. Phys. **15**(6), 643–662 (2003)
9. Ruskai, M.B.: Open problems in quantum information theory, pp. 1–21 (2007, preprint) arXiv:0708.1902
10. Stinespring, W.F.: Positive functions on C^*-algebras. Proc. Am. Math. Soc. **6**, 211–216 (1955)