Separability and Entanglement-Breaking in Infinite Dimensions

A. S. Holevo*†, M. E. Shirokov* and R. F. Werner‡

1 Introduction

In this paper we give a general integral representation for separable states in the tensor product of infinite dimensional Hilbert spaces and provide the first example of separable states that are not countably decomposable. We also prove the structure theorem for the quantum communication channels that are entanglement-breaking, generalizing the finite-dimensional result of M. Horodecki, Ruskai and Shor. In the finite dimensional case such channels can be characterized as having the Kraus representation with operators of rank 1. The above example implies existence of infinite-dimensional entanglement-breaking channels having no such representation.

2 Separable states

In what follows $\mathcal{H}, \mathcal{K}, \dots$ denote separable Hilbert spaces; $\mathfrak{T}(\mathcal{H})$ denotes the Banach space of trace-class operators in $\mathcal{H}$, and $\mathfrak{S}(\mathcal{H})$ – the convex subset of all density operators. We shall also call them *states* for brevity, having in mind that a density operator ρ uniqiely determines a normal state on the algebra of all bounded operators in $\mathcal{H}$. Equipped with the trace-norm distance, $\mathfrak{S}(\mathcal{H})$ is a complete separable metric space. It is known [2], [3]

*Steklov Mathematical Institute, Moscow, Russia.

†Part of this work was done when the author was visiting the Institute of Mathematical Physics, TU Braunschweig in frame of the A. von Humboldt Foundation Follow-up Program.

‡Institute of Mathematical Physics, TU Braunschweig.

that a sequence of quantum states converging to a state in the weak operator topology converges to it in the trace norm.

If π is a Borel probability measure on $\mathfrak{S}(\mathcal{H})$, the relation

$$\bar{\rho}(\pi)=\int_{\mathfrak{S}(\mathcal{H})}\sigma\pi(d\sigma), \tag{1}$$

where the integral exists as Bochner integral, defines a state called *barycenter* of π. Let $\mathcal{P}$ be a set of Borel probability measures on $\mathfrak{S}(\mathcal{H})$. Recall that weak convergence of probability measures means convergence of integrals of all continuous bounded functions (see e. g. [8]). By using the above mentioned result in [2], [3] it is easy to see that the map $\pi\mapsto\bar{\rho}(\pi)$ from $\mathcal{P}$ onto $\mathfrak{S}(\mathcal{H})$ is continuous. The following result was established in [5]:

Theorem 1. *The set $\mathcal{P}$ is weakly compact if and only if its image $\mathcal{A}$ under the map $\pi\mapsto\bar{\rho}(\pi)$ given by (1) is a compact subset of $\mathfrak{S}(\mathcal{H})$.*

The following lemma is an amplified version of the Choquet decomposition [1] adapted to the case of closed convex subsets of $\mathfrak{S}(\mathcal{H})$. We denote by $\mathrm{co}\mathcal{A}$ ($\overline{\mathrm{co}}\mathcal{A}$) the convex hull (closure) of a set $\mathcal{A}$ [7].

Lemma 1. *Let $\mathcal{A}$ be a closed subset of $\mathfrak{S}(\mathcal{H})$. Then $\overline{\mathrm{co}}\mathcal{A}$ coincides with the set of barycenters of all Borel probability measures supported by $\mathcal{A}$.*

Proof. Let $\rho_0\in\overline{\mathrm{co}}\mathcal{A}$. Then there is a sequence $\{\rho_n\}\subseteq\mathrm{co}\mathcal{A}$ converging to ρ_0, so that $\{\rho_n\}$ is relatively compact in $\mathfrak{S}(\mathcal{H})$. The density operator ρ_n is barycenter of Borel probability measure π_n finitely supported on $\mathcal{A}$. By the compactness criterion of theorem 1, the sequence $\{\pi_n\}$ is weakly relatively compact and thus has a partial limit π_0, which is supported by the set $\mathcal{A}$ due to theorem 6.1 in [8]. Continuity of the map $\pi\mapsto\bar{\rho}(\pi)=\int\sigma\pi(d\sigma)$ implies that the state ρ_0 is the barycenter of the measure π_0.

Conversely, let π be an arbitrary probability measure supported by $\mathcal{A}$. By theorem 6.3[1] in [8] this measure can be weakly approximated by a sequence of measures π_n finitely supported by $\mathcal{A}$. Since $\bar{\rho}(\pi_n)$ is in $\mathrm{co}\mathcal{A}$ for all n we conclude that $\bar{\rho}(\pi)$ is in $\overline{\mathrm{co}}\mathcal{A}$ due to continuity of the map $\pi\mapsto\bar{\rho}(\pi)$. $\square$

Definition 1. *A state in $\mathfrak{S}(\mathcal{H}\otimes\mathcal{K})$ is called separable if it is in the convex closure of the set of all product states in $\mathfrak{S}(\mathcal{H}\otimes\mathcal{K})$.*

Lemma 1 implies that separable states are precisely those states which admit the representation

$$\rho=\int_{\mathfrak{S}(\mathcal{H})}\int_{\mathfrak{S}(\mathcal{K})}(\rho_{\mathcal{H}}\otimes\rho_{\mathcal{K}})\,\mu(d\rho_{\mathcal{H}}d\rho_{\mathcal{K}}), \tag{2}$$

[1] More precisely, it follows from the construction used in the proof of this theorem.

where μ is a Borel probability measure on $\mathfrak{S}(\mathcal{H}) \times \mathfrak{S}(\mathcal{K})$. In the finite dimensional case application of Caratheodory's theorem reduces this to the familiar definition of separable state as finite convex combination of product states [11]. If for a separable state ρ it is possible to find a representation (2) with purely atomic μ, we call the state *countably decomposable.* A necessary condition for this is existence of nonzero vectors $|\alpha\rangle \in \mathcal{H}, |\beta\rangle \in \mathcal{K}$ such that

$$\rho \geq |\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|, \tag{3}$$

cf. [12]. In Sec. 2 we shall show that there are many separable states which do not satisfy this condition and hence are not countably decomposable.

In the definition 1 one can replace the set of all product states by the set of all products of pure states. It is known that the subset $\mathfrak{P}(\mathcal{H})$ of pure states (extreme points of $\mathfrak{S}(\mathcal{H})$) is closed in the trace-norm topology. The lemma 1 then implies that a state ρ is separable if and only if there is a Borel measure ν on $\mathfrak{P}(\mathcal{H}) \times \mathfrak{P}(\mathcal{K})$ such that, with some abuse of notation,

$$\rho = \int_{\mathfrak{P}(\mathcal{H})} \int_{\mathfrak{P}(\mathcal{K})} |\varphi\rangle\langle\varphi| \otimes |\psi\rangle\langle\psi| \nu(d\varphi d\psi). \tag{4}$$

3 Entanglement-breaking channels

A *channel* is a linear map $\Phi{:}\mathfrak{T}(\mathcal{H}) \mapsto \mathfrak{T}(\mathcal{H}')$ with the properties:

1) $\Phi(\mathfrak{S}(\mathcal{H})) \subseteq \mathfrak{S}(\mathcal{H}')$; this implies that Φ is bounded map and hence is uniquely determined by the infinite matrix $[\Phi(|i\rangle\langle j|)]$, where $\{|i\rangle\}$ is an orthonormal basis in $\mathcal{H}$.

2) The matrix $[\Phi(|i\rangle\langle j|)]$ is positive definite in the sense that for a collection of vectors $\{|\psi_i\rangle\} \subseteq \mathcal{H}$ with finite number of nonzero elements

$$\sum_{ij} \langle\psi_i|\Phi(|i\rangle\langle j|)|\psi_j\rangle \geq 0. \tag{5}$$

Definition 2. *A channel Φ is called entanglement-breaking if for arbitrary Hilbert space $\mathcal{K}$ and arbitrary state $\omega \in \mathfrak{S}(\mathcal{H}\otimes\mathcal{K})$ the state $(\Phi\otimes\mathrm{Id}_{\mathcal{K}})(\omega)$, where $\mathrm{Id}_{\mathcal{K}}$ is the identity channel in $\mathfrak{S}(\mathcal{K})$, is separable.*

Note that in this definition one can restrict to finite dimensional Hilbert spaces $\mathcal{K}$. Indeed, an arbitrary state ω in $\mathfrak{S}(\mathcal{H}\otimes\mathcal{K})$ with an infinite dimensional $\mathcal{K}$ can be approximated by the states

$$\omega_n = (\mathrm{Tr}(I_{\mathcal{H}} \otimes Q_n)\omega)^{-1}(I_{\mathcal{H}} \otimes Q_n)\omega(I_{\mathcal{H}} \otimes Q_n),$$

where $\{Q_n\}$ is the sequence of the spectral projectors of the partial state $\mathrm{Tr}_{\mathcal{H}}\omega$ corresponding to its n largest eigenvalues. Each state ω_n can be considered as a state in $\mathfrak{S}(\mathcal{H}\otimes\mathcal{K}_n)$, where $\mathcal{K}_n = Q_n(\mathcal{K})$ is n-dimensional Hilbert space. If $(\Phi\otimes\mathrm{Id})(\omega_n)$ is separable for all n, then $(\Phi\otimes\mathrm{Id})(\omega)$ is also separable as a limit of sequence of separable states.

The following theorem is a generalization of the result in [6] to the infinite dimensional case.

Theorem 2. *Channel Φ is entanglement-breaking if and only if there is a complete separable metric space $\mathcal{X}$, a Borel $\mathfrak{S}(\mathcal{H}')$-valued function $x\mapsto\rho'(x)$ and a positive operator-valued Borel measure (POVM) $M(dx)$ on $\mathcal{X}$ such that*

$$\Phi(\rho) = \int\limits_{\mathcal{X}} \rho'(x)\mu_\rho(dx), \tag{6}$$

where $\mu_\rho(B) = \mathrm{Tr}\rho M(B)$ for all Borel $B\subseteq\mathcal{X}$.

Proof. Notice first that conditions 1),2) in the definition of channel are readily verified for the map (6). Let us show that the channel (6) is entanglement-breaking. Let $\omega\in\mathfrak{S}(\mathcal{H}\otimes\mathcal{K})$, where $\mathcal{K}$ is a finite dimensional Hilbert space. We have

$$(\Phi\otimes\mathrm{Id}_{\mathcal{K}})(\omega) = \int\limits_{\mathcal{X}} \rho'(x)\otimes m_\omega(dx), \tag{7}$$

where

$$m_\omega(B) = \mathrm{Tr}_{\mathcal{H}}\omega(M(B)\otimes I_{\mathcal{K}}), \quad B\subseteq\mathcal{X}.$$

It is easy to see that any matrix element of m_ω (in a particular basis) is a complex valued measure on $\mathcal{X}$ absolutely continuous with respect to the probability measure $\mu_\omega(B) = \mathrm{Tr}m_\omega(B)$, $B\subseteq\mathcal{X}$. The Radon-Nikodym theorem implies representation

$$m_\omega(B) = \int\limits_{B} \sigma_\omega(x)\mu_\omega(dx),$$

where $\sigma_\omega(x)$ is a function on $\mathcal{X}$ taking values in $\mathfrak{S}(\mathcal{K})$. By using this representation we can rewrite (7) as

$$(\Phi\otimes\mathrm{Id}_{\mathcal{K}})(\omega) = \int\limits_{\mathcal{X}} \rho'(x)\otimes\sigma_\omega(x)\mu_\omega(dx), \tag{8}$$

which reduces to (2) by change of variables and hence is separable by Lemma 1.

Conversely, let Φ be an entanglement-breaking channel. Fix a state σ in $\mathfrak{S}(\mathcal{H})$ of full rank and let $\{|i\rangle\}_{i=1}^{+\infty}$ be the basis of eigenvectors of σ with the corresponding (positive) eigenvalues $\{\lambda_i\}_{i=1}^{+\infty}$. Consider the vector

$$|\Omega\rangle = \sum_{i=1}^{+\infty} \lambda_i^{1/2} |i\rangle \otimes |i\rangle$$

in the space $\mathcal{H} \otimes \mathcal{H}$. Since Φ is entanglement-breaking, the state

$$\rho = (\mathrm{Id}_{\mathcal{H}} \otimes \Phi)(|\Omega\rangle\langle\Omega|) \tag{9}$$

in $\mathfrak{S}(\mathcal{H} \otimes \mathcal{H}')$ is separable. By (4) there exists a probability measure ν on $\mathfrak{P}(\mathcal{H}) \times \mathfrak{P}(\mathcal{H}')$ such that

$$(\mathrm{Id}_{\mathcal{H}} \otimes \Phi)(|\Omega\rangle\langle\Omega|) = \int\limits_{\mathfrak{P}(\mathcal{H})} \int\limits_{\mathfrak{P}(\mathcal{H}')} |\varphi\rangle\langle\varphi| \otimes |\psi\rangle\langle\psi| \nu(d\varphi d\psi). \tag{10}$$

This implies

$$\begin{aligned} \sigma &= \mathrm{Tr}_{\mathcal{H}'}(Id_{\mathcal{H}} \otimes \Phi)(|\Omega\rangle\langle\Omega|) \\ &= \int\limits_{\mathfrak{P}(\mathcal{H})} \int\limits_{\mathfrak{P}(\mathcal{H}')} |\varphi\rangle\langle\varphi| \nu(d\varphi d\psi) \\ &= \int\limits_{\mathfrak{P}(\mathcal{H})} \int\limits_{\mathfrak{P}(\mathcal{H}')} |\bar{\varphi}\rangle\langle\bar{\varphi}| \nu(d\varphi d\psi), \end{aligned} \tag{11}$$

where the bar denotes complex conjugation in the basis$\{|i\rangle\}_{i=1}^{+\infty}$. By this equality for arbitrary Borel $B \subseteq \mathfrak{P}(\mathcal{H}')$ the operator

$$M(B) = \sigma^{-1/2} \left[\int\limits_{\mathfrak{P}(\mathcal{H})} \int\limits_{B} |\bar{\varphi}\rangle\langle\bar{\varphi}| \nu(d\varphi d\psi) \right] \sigma^{-1/2}$$

can be defined as a bounded positive operator on $\mathcal{H}$ such that $M(B) \leq M(\mathcal{X}) = I_{\mathcal{H}}$. It is easy to see that $M(d\psi)$ is a POVM on $\mathcal{X} = \mathfrak{P}(\mathcal{H}')$.

Consider the entanglement-breaking channel

$$\hat{\Phi}(\rho) = \int\limits_{\mathfrak{P}(\mathcal{H}')} |\psi\rangle\langle\psi|\mu_\rho(d\psi),$$

where μ_ρ is the Borel probability measure defined by $\mu_\rho(B) = \mathrm{Tr}\rho M(B), B \subseteq \mathcal{X}$. To prove that $\Phi(\rho) = \hat{\Phi}(\rho)$, it is sufficient to show that

$$\hat{\Phi}(|i\rangle\langle j|) = \Phi(|i\rangle\langle j|)$$

for all i, j. But

$$\hat{\Phi}(|i\rangle\langle j|) = \int\limits_{\mathfrak{P}(\mathcal{H}')} |\psi\rangle\langle\psi|\langle j|M(d\psi)|i\rangle$$
$$= \lambda_i^{-1/2}\lambda_j^{-1/2} \int\limits_{\mathfrak{P}(\mathcal{H})} \int\limits_{\mathfrak{P}(\mathcal{H}')} \langle i|\varphi\rangle\langle\varphi|j\rangle|\psi\rangle\langle\psi|\nu(d\varphi d\psi) = \Phi(e_{ij}),$$

where

$$e_{ij} = \lambda_i^{-1/2}\lambda_j^{-1/2}\mathrm{Tr}_{\mathcal{H}}(|j\rangle\langle i| \otimes I)|\Omega\rangle\langle\Omega| = |i\rangle\langle j|. \quad \square$$

The representation (6) is by no means unique. A natural question is: for an arbitrary entanglement-breaking channel, is it possible to find a representation (6) with a purely atomic POVM? From the proof of the theorem one can see that this is the case if and only if the state (9) is countably decomposable, hence, as we show in the next section, the answer is negative. This implies existence of an entanglement-breaking channel, which has no Kraus representation with operators of rank 1, in contrast to the finite dimensional case [6]. Indeed, it is easy to see that such a Kraus representation with operators of rank 1 is equivalent to a representation (6) of this channel with a purely atomic POVM.

4 Example

We shall consider the one-dimensional rotation group represented as the interval $[0, 2\pi)$ with addition mod2π. Let $\mathcal{H} = L^2\ [0, 2\pi)$ with the normalized Lebesgue measure $\frac{dx}{2\pi}$, and let $\{|k\rangle; k \in \mathbf{Z}\}$ be the orthonormal basis of trigonometric functions, so that

$$\langle k|\psi\rangle = \int_0^{2\pi} e^{-ixk}\psi(x)\frac{dx}{2\pi}.$$

Consider the unitary representation $x \to V_x$, where $V_x = \sum_{-\infty}^{\infty} e^{ixk}|k\rangle\langle k|$, so that $(V_u\psi)(x) = \psi(x-u)$. For any fixed state vector $|\varphi\rangle \in \mathcal{H}$, the formula

$$\Phi(\rho) = \int_0^{2\pi} V_x|\varphi\rangle\langle\varphi|V_x^* \mu_\rho(dx), \tag{12}$$

where $\mu_\rho(B) = \mathrm{Tr}\rho E(B)$, and $E(dx)$ is the spectral measure of the operator of multiplication by x in $\mathcal{H} = L^2[0, 2\pi)$, defines entanglement–breaking channel. The channel Φ is rotation-covariant in that

$$\Phi(V_x\rho V_x^*) = V_x\Phi(\rho)V_x^*, \qquad x \in [0, 2\pi). \tag{13}$$

It is not difficult to check that

$$\mu_\rho(B) = \int_B \langle x|\rho|x\rangle \frac{dx}{2\pi}, \tag{14}$$

where $\langle x|\rho|x\rangle = p(x)$ is the diagonal value of the density operator ρ which is unambiguously defined as a probability density in L^1.

Theorem 3. *For arbitrary state vectors $|\varphi_j\rangle \in \mathcal{H}_j \simeq L^2[0; 2\pi); j = 1, 2,$ with nonvanishing Fourier coefficients the separable state*

$$\rho_{12} = \int_0^{2\pi} V_x^{(1)}|\varphi_1\rangle\langle\varphi_1|V_x^{(1)*} \otimes V_x^{(2)}|\varphi_2\rangle\langle\varphi_2|V_x^{(2)*} \frac{dx}{2\pi} \tag{15}$$

in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is not countably decomposable.

Proof. Suppose ρ is countably decomposable, then by (3) there exist nonzero $\alpha_j \in \mathcal{H}_j$ such that

$$\rho_{12} \geq |\alpha_1\rangle\langle\alpha_1| \otimes |\alpha_2\rangle\langle\alpha_2|. \tag{16}$$

Taking partial traces we obtain

$$\int_0^{2\pi} V_x^{(j)}|\varphi_j\rangle\langle\varphi_j|V_x^{(j)*} \frac{dx}{2\pi} \geq |\alpha_j\rangle\langle\alpha_j|,$$

whence

$$|\langle k|\varphi_j\rangle| \geq |\langle k|\alpha_j\rangle|; \quad j = 1, 2; \quad k \in \mathbb{Z}. \tag{17}$$

Inequality (16) means that

$$\int_0^{2\pi} \left|\langle\lambda_1|V_x^{(1)}|\varphi_1\rangle\right|^2 \left|\langle\lambda_2|V_x^{(2)}|\varphi_2\rangle\right|^2 \frac{dx}{2\pi} \geq |\langle\lambda_1|\alpha_1\rangle|^2 |\langle\lambda_2|\alpha_2\rangle|^2 \tag{18}$$

for arbitrary $\lambda_j \in L^2[0;2\pi)$. For technical convenience we will assume that the functions $\lambda_j(x)$ have finite number of nonzero Fourier coefficients. Introducing

$$\mu_j(x) = \langle \lambda_j | V_x^{(j)} | \varphi_j \rangle = \sum_{k=-\infty}^{+\infty} \langle \lambda_j | k \rangle \langle k | \varphi_j \rangle e^{ikx},$$

so that $\langle k | \mu_j \rangle = \langle \lambda_j | k \rangle \langle k | \varphi_j \rangle$, we see that $\mu_j \mapsto \langle \lambda_j | \alpha_j \rangle$ are linear functionals of μ_j running over the subspace of trigonometric polynomials in $L^2[0;2\pi)$. These functional are in fact continuous. Indeed, choosing k such that $\langle k | \alpha_2 \rangle \neq 0$, we find from (18)

$$|\langle \lambda_1 | \alpha_1 \rangle|^2 \leq \left| \frac{\langle k | \varphi_2 \rangle}{\langle k | \alpha_2 \rangle} \right|^2 \int_0^{2\pi} |\mu_1(x)|^2 \, \frac{dx}{2\pi}$$

for all trigonometric polynomials μ_1. Hence by Riesz theorem there exists $\beta_1 \in L^2[0;2\pi)$ such that $\langle \lambda_1 | \alpha_1 \rangle = \langle \beta_1 | \mu_1 \rangle$. Applying similar reasoning to $j = 2$, we can transform (18) to the form

$$|\langle \beta_1 | \mu_1 \rangle|^2 |\langle \beta_2 | \mu_2 \rangle|^2 \leq \int_0^{2\pi} |\mu_1(x) \mu_2(x)|^2 \, \frac{dx}{2\pi}, \tag{19}$$

where $\beta_j \in L^2[0;2\pi)$.

Now we can extend the inequality (19) to more general functions μ_j for which both sides of this inequality are defined e. g. measurable a. e. uniformly bounded functions on $[0;2\pi]$. The characteristic functions of intervals belong to this class, and so is a dense set of functions with support in any specified interval.

Consider a partitioning of the interval $[0, 2\pi]$ into intervals of length $\leq \varepsilon$, and pick one of these intervals, say I_2, on which β_2 is not a.e. zero. Then we can find an admissible function μ_2 supported in I_2 such that $\langle \beta_2 | \mu_2 \rangle \neq 0$. But then, for any μ_1 supported on the complement of I_2, the right hand side of (19) vanishes, and therefore β_1 vanishes a.e. on the complement of I_2. It follows that the support of β_1 has measure $\leq \varepsilon$ for all ε, i.e., β_1 vanishes a.e., and hence $\alpha_1 = 0$. □

Let $\mathfrak{W}$ be the subset of all separable states which are not countably decomposable.

Corollary. *An arbitrary pure product state in $\mathfrak{S}(\mathcal{H} \otimes \mathcal{K})$ can be approximated by a sequence from $\mathfrak{W}$.*

Proof. We can take $\mathcal{H},\mathcal{K}\simeq L^2[0;2\pi)$. Since an arbitrary function in L^2 can be approximated by functions with nonzero Fourier coefficients it sufficient to consider pure product state $|\varphi_1\rangle\langle\varphi_1|\otimes|\varphi_2\rangle\langle\varphi_2|$, where $\varphi_j(x)$ have this property.

Consider the sequence of states

$$\rho_{12}^{(n)}=\int_0^{2\pi/n}V_x^{(1)}|\varphi_1\rangle\langle\varphi_1|V_x^{(1)*}\otimes V_x^{(2)}|\varphi_2\rangle\langle\varphi_2|V_x^{(2)*}\,\frac{ndx}{2\pi},$$

such that $\rho_{12}^{(n)}\to|\varphi_1\rangle\langle\varphi_1|\otimes|\varphi_2\rangle\langle\varphi_2|$ as $n\to\infty$. For the state ρ_{12} given by the (15), we have

$$\rho_{12}=\frac{1}{n}\sum_{k=0}^{n-1}\left(V_{\frac{2\pi k}{n}}^{(1)}\otimes V_{\frac{2\pi k}{n}}^{(2)}\right)\rho_{12}^{(n)}\left(V_{\frac{2\pi k}{n}}^{(1)}\otimes V_{\frac{2\pi k}{n}}^{(2)}\right)^*,$$

therefore $\rho_{12}^{(n)}\in\mathfrak{W}$. Indeed, otherwise we could construct a countable decomposition for ρ_{12}. $\square$

Conjecture. *The subset $\mathfrak{W}$ is dense in the set of all separable states.*

5 The classical capacity

In terms of the relative entropy, the $\chi-$capacity of an arbitrary quantum channel Φ is defined by the relation

$$C(\Phi)=\sup_{\{\pi_i,\rho_i\}}\sum_i\pi_iH(\Phi(\rho_i);\Phi(\bar{\rho})),\tag{20}$$

where supremum is over all (finite) ensembles $\{\pi_i,\rho_i\}$ with the average $\bar{\rho}$. For entanglement-breaking channels the χ- capacity is additive (for the infinite-dimensional case see [9]), hence it gives the classical capacity of the channel.

Theorem 4. *The classical capacity of the channel (12) is equal to*

$$C(\Phi)=-\sum_{k=-\infty}^{\infty}|\langle k|\varphi\rangle|^2\log|\langle k|\varphi\rangle|^2.\tag{21}$$

Proof. Let us first show that the closure of $\mathrm{ran}\Phi=\Phi\left(\mathfrak{S}(\mathcal{H})\right)$ coincides with the set

$$\overline{\mathrm{co}}\left\{V_x|\varphi\rangle\langle\varphi|V_x^*;x\in[0,2\pi]\right\}.\tag{22}$$

By (14) and using the fact that arbitrary probability density $p(\cdot)$ can be obtained as the diagonal value of a density operator (in fact, of a pure state), we have

$$\mathrm{ran}\Phi = \left\{ \int_0^{2\pi} V_x|\varphi\rangle\langle\varphi|V_x^* p(x) \frac{dx}{2\pi}; \quad p(\cdot) \in \mathcal{P} \right\}, \tag{23}$$

where $\mathcal{P}$ is the convex set of probability densities on $[0, 2\pi]$. The set of absolutely continuous probability measures is weakly dense in the Choquet simplex $\mathcal{M}$ of all Borel probability measures on $[0, 2\pi]$, while the map

$$\mu \mapsto \int_0^{2\pi} V_x|\varphi\rangle\langle\varphi|V_x^* \mu(dx)$$

is continuous (due to the aforementioned result in [2], [3]), therefore the set (23) is dense in the compact convex set

$$\left\{ \int_0^{2\pi} V_x|\varphi\rangle\langle\varphi|V_x^* \mu(dx); \ \mu \in \mathcal{M} \right\},$$

which coincides with the set (22) by lemma 1.

Now suppose $C(\Phi)$ is finite. By proposition 1 in [9] there exists the unique state $\Omega(\Phi)$ in $\overline{\mathrm{ran}}\Phi$ such that

$$C(\Phi) = \sup_{\rho \in \mathfrak{S}(\mathcal{H})} H(\Phi(\rho); \Omega(\Phi)). \tag{24}$$

The uniqueness of this state and the covariance (13) imply $V_x \Omega(\Phi) V_x^* = \Omega(\Phi)$ for all x and hence

$$\Omega(\Phi) = \int_0^{2\pi} V_x|\varphi\rangle\langle\varphi|V_x^* \frac{dx}{2\pi} = - \sum_{k=-\infty}^{\infty} |\langle k|\varphi\rangle|^2 |k\rangle\langle k|.$$

Since $\mathrm{ran}\Phi$ is dense in the set (22), and the relative entropy is lower semicontinuous and convex, we see that the supremum (24) is equal to $H(|\varphi\rangle\langle\varphi|; \Omega(\Phi))$, so we have

$$C(\Phi) = -\langle\varphi| \log \Omega(\Phi) |\varphi\rangle = H\left(\Omega(\Phi)\right)$$

which is equal to the right side of (21).

To complete the proof it is sufficient to show that

$$- \sum_{k=-\infty}^{\infty} |\langle k|\varphi\rangle|^2 \log |\langle k|\varphi\rangle|^2 < \infty \tag{25}$$

implies finiteness of the capacity $C(\Phi)$. Let us show first that (25) implies continuity of the output entropy $H(\Phi(\rho))$. Indeed, assuming (25) one can find a sequence $\{h_k\}$ of positive numbers such that $h_k \uparrow +\infty$ with $|k| \uparrow +\infty$ and

$$\sum_{k=-\infty}^{+\infty} h_k |\langle k|\varphi\rangle|^2 (-\log |\langle k|\varphi\rangle|^2) \equiv h < \infty.$$

Introducing selfadjoint operator

$$H = \sum_{k=-\infty}^{+\infty} h_k (-\log |\langle k|\varphi\rangle|^2) |k\rangle\langle k|,$$

we have

$$\mathrm{Tr}\exp(-\beta H) = \sum_{k=-\infty}^{+\infty} |\langle k|\varphi\rangle|^{2\beta h_k} < \infty; \quad \beta > 0, \tag{26}$$

since $\beta h_k \geq 1$ for all sufficiently large k. By (23), for arbitrary $\rho \in \overline{\mathrm{ran}}\Phi$ there is a probability measure μ such that $\rho = \int_0^{2\pi} V_x |\varphi\rangle\langle\varphi| V_x^* \mu(dx)$. Thus

$$\mathrm{Tr}\rho H = \sum_{k=-\infty}^{+\infty} h_k |\langle k|\varphi\rangle|^2 (-\log |\langle k|\varphi\rangle|^2) \int_0^{2\pi} \mu(dx) = h \tag{27}$$

for $\rho \in \overline{\mathrm{ran}}\Phi$. It is well known [10] that the relations (26) and (27) imply continuity of the restriction of the quantum entropy to the set $\overline{\mathrm{ran}}\Phi$, which implies continuity of the output entropy $H(\Phi(\rho))$ on $\mathfrak{S}(\mathcal{H})$.

Now the maximum of the quantum entropy on the set $\overline{\mathrm{ran}}\Phi$ is attained on the state $\Omega(\Phi)$ and is equal to the sum of the series (25). Indeed, by the unitary invariance, concavity and continuity of the output entropy, we have

$$H(\rho\prime) = \int_0^{2\pi} H(V_x \rho\prime V_x^*) \frac{dx}{2\pi} \leq H\left(\int_0^{2\pi} V_x \rho\prime V_x^* \frac{dx}{2\pi}\right) = H(\Omega(\Phi))$$

for any $\rho\prime \in \overline{\mathrm{ran}}\Phi$. Therefore

$$C(\Phi) \leq \max_{\rho} H(\Phi(\rho)) = H(\Omega(\Phi)) < \infty.$$

Moreover, continuity of the entropy on the set $\overline{\mathrm{ran}}\Phi$, which is the convex closure of a family of pure states, implies $\inf_\rho H(\Phi(\rho)) = 0$ and $C(\Phi) = \max_\rho H(\Phi(\rho))$. $\square$

References

[1] Alfsen E., “Compact convex sets and boundary integrals” , Springer Verlag, 1971.

[2] Davies, E.B. “Quantum stochastic processes-I”, Comm. Math. Phys., 15, 277-304, 1969.

[3] Dell’Antonio G.F., “On the limits of sequences of states”, Commun. Pure Appl. Math. 20, 413-430, 1967;

[4] Holevo, A. S., “Classical capacities of quantum channels with constrained inputs”, Probability Theory and Applications, 48, N.2, 359-374, 2003, e-print quant-ph/0211170;

[5] Holevo, A.S., Shirokov M.E., “Continuous ensembles and the χ-capacity of infinite dimensional channels”, Probability Theory and Applications, 50, N.1, 98-114, 2005, LANL e-print quant-ph/0408176;

[6] Horodecki M., Shor P.W., Ruskai, M.B. “General Entanglement Breaking Channels”, Rev. Math. Phys. 15, 629-641, 2003, LANL e-print quant-ph/0302031;

[7] Joffe, A. D., Tikhomirov, W. M.: “Theory of extremum problems”, AP, NY, 1979;

[8] Parthasarathy, K., “Probability measures on metric spaces”, Academic Press, New York and London, 1967;

[9] Shirokov, M.E., “The Holevo capacity of infinite dimensional channels”, e-print quant-ph/0408009, 2004;

[10] Wehrl, A., “General properties of entropy”, Rev. Mod. Phys. 50, 221-250, 1978;

[11] Werner, R.F., “Quantum harmonic ocsillator in phase space”, J. Math. Phys., V.25, 1404-1411, 1984;

[12] Werner, R.F., Wolf, M. M., “Bound entangled Gaussian states”, e-print quant-ph/0009118.