ELSEVIER

A fidelity measure for quantum channels

Maxim Raginsky

*Center for Photonic Communication and Computing, Department of Electrical and Computer Engineering, Northwestern University,
Evanston, IL 60208-3118, USA*

Abstract

We propose a fidelity measure for quantum channels in a straightforward analogy to the corresponding mixed-state fidelity of Jozsa. We describe properties of this fidelity measure and discuss some applications of it to quantum information science. © 2001 Elsevier Science B.V. All rights reserved.

1. Introduction

Given any pair ρ, σ of density operators, the fidelity [1]

$$F(\rho, \sigma) := \left(\mathrm{tr} \sqrt{\sqrt{\rho}\, \sigma \sqrt{\rho}} \right)^2 \qquad (1)$$

quantifies the extent to which ρ and σ can be distinguished from one another. The properties it possesses are quite natural from the physical point of view. For instance, $0 \leqslant F(\rho, \sigma) \leqslant 1$, and $F(\rho, \sigma) = 1$ if and only if $\rho = \sigma$; for any unitary transformation U, [1] $F(U \rho U^*, U \sigma U^*) = F(\rho, \sigma)$; and, according to a theorem of Uhlmann [1,2],

$$F(\rho, \sigma) = \max_{|\psi_\rho\rangle, |\psi_\sigma\rangle} \left| \langle \psi_\rho | \psi_\sigma \rangle \right|^2, \qquad (2)$$

where $|\psi_\rho\rangle$ and $|\psi_\sigma\rangle$ are purifications of ρ and σ on an extended Hilbert space. Furthermore, fidelity (1) is known to be equivalent to other measures of distinguishability of quantum states [3].

In a paper of Childs et al. [4] it was suggested that a notion of distinguishability for quantum channels would be as vital to quantum information science as the corresponding notion for quantum states. (We recall that a quantum channel between two systems with Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, respectively, is a completely positive trace-preserving linear map from the set $\mathcal{S}(\mathcal{H})$ of density operators on $\mathcal{H}$ to the set $\mathcal{S}(\mathcal{K})$ of density operators on $\mathcal{K}$.) In this Letter we show that a fidelity measure for a pair of quantum channels S and T can be derived from fidelity (1) for suitably chosen density operators ρ_S and ρ_T, and that the proposed fidelity measure enjoys properties that are quite similar to those of the mixed-state fidelity. We also prove an analogue of Uhlmann's theorem, formulated in terms of dilations of channels on an extended Hilbert space. We then discuss our fidelity measure in the context of

---

E-mail address: maxim@northwestern.edu (M. Raginsky).

[1] In this Letter, given an operator X, the adjoint operator will be denoted by X^*, not $X^\dagger$.

(a) distinguishing channels via superdense coding, (b) improving distinguishability of channels through pre-processing, and (c) characterizing the performance of quantum error-correcting codes.

2. Duality between quantum channels and bipartite states

In order to state our results in clear and compact form, we briefly recall a very convenient characterization of quantum channels by means of bipartite states. Let T be a channel that converts systems with the finite-dimensional Hilbert space $\mathcal{H}$ into systems with the finite-dimensional Hilbert space $\mathcal{K}$. It is well-known that the action of T can be described by giving its *Kraus operators*, $V_\alpha : \mathcal{H} \to \mathcal{K}$, so that, for any density operator $\rho \in \mathcal{S}(\mathcal{H})$,

$$T(\rho) = \sum_\alpha V_\alpha \rho V_\alpha^*. \tag{3}$$

Since T is trace-preserving, the Kraus operators must satisfy the relation

$$\sum_\alpha V_\alpha^* V_\alpha = \mathbb{1}_{\mathcal{H}}. \tag{4}$$

The Kraus representation (3) is unique only up to unitary equivalence, and thus does not provide a one-to-one characterization of channels. One such characterization was described in Ref. [5]. Given a channel $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$ with $\dim \mathcal{H} = d < \infty$, we define an operator R_T on $\mathcal{K} \otimes \mathcal{H}$ through

$$R_T := (T \otimes \mathrm{id}) |\varphi_{\mathcal{H}}^+\rangle\langle\varphi_{\mathcal{H}}^+|, \tag{5}$$

where "id" denotes the identity channel, and $|\varphi_{\mathcal{H}}^+\rangle \in \mathcal{H}^{\otimes 2}$ is the unnormalized maximally entangled state $\sum_{i=1}^d |e_i\rangle \otimes |e_i\rangle$. Then the action of T on an arbitrary density operator ρ on $\mathcal{H}$ is given by

$$T(\rho) = \mathrm{tr}_{\mathcal{H}}\big[(\mathbb{1} \otimes \rho^\top) R_T\big], \tag{6}$$

where $\rho^\top$ denotes the transpose of ρ in the basis $\{|e_i\rangle\}$. We must be careful with Eq. (6) because (a) the subscript $\mathcal{H}$ refers to the *second* factor in the tensor product, since both $\mathbb{1} \otimes \rho^\top$ and R_T are operators that act on $\mathcal{K} \otimes \mathcal{H}$; and (b) all matrix operations (e.g., the transpose) refer to the basis which has been fixed beforehand, when defining R_T. It turns out that the correspondence $T \mapsto R_T$ is one-to-one, i.e., $R_S = R_T$ if

and only if $S = T$ (see Ref. [5] for a detailed discussion). The requirement for T to be trace-preserving translates into [5]

$$\mathrm{tr}_{\mathcal{K}} R_T = \mathbb{1}_{\mathcal{H}}. \tag{7}$$

This formalism can be extended to channels acting on bipartite systems [6]. Let T be a channel that maps states on $\mathcal{H}_1 \otimes \mathcal{H}_2$ to states on $\mathcal{K}_1 \otimes \mathcal{K}_2$ (here we assume, for simplicity, that $\dim \mathcal{H}_1 = \dim \mathcal{H}_2 = d$). Then we define

$$R_T := (T_{\mathrm{odd}} \otimes \mathrm{id}_{\mathrm{even}})\big(|\varphi_{\mathcal{H}_1}^+\rangle\langle\varphi_{\mathcal{H}_1}^+| \otimes |\varphi_{\mathcal{H}_2}^+\rangle\langle\varphi_{\mathcal{H}_2}^+|\big), \tag{8}$$

where $T_{\mathrm{odd}} \otimes \mathrm{id}_{\mathrm{even}}$ signifies that the channel T acts only on odd-numbered factors of $|\varphi_{\mathcal{H}_1}^+\rangle\langle\varphi_{\mathcal{H}_1}^+| \otimes |\varphi_{\mathcal{H}_2}^+\rangle\langle\varphi_{\mathcal{H}_2}^+|$, while the identity channel acts on even-numbered factors. The operator R_T defined in Eq. (8) acts on $\mathcal{K}_1 \otimes \mathcal{H}_1 \otimes \mathcal{K}_2 \otimes \mathcal{H}_2$, and the action of the channel T on any $\rho \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is given by

$$T(\rho) = \mathrm{tr}_{\mathcal{H}_1 \mathcal{H}_2}\big[\big(\mathbb{1}_{\mathcal{K}_1 \otimes \mathcal{K}_2} \otimes \rho^\top_{\mathcal{H}_1 \otimes \mathcal{H}_2}\big) R_T\big]. \tag{9}$$

All of the above relations can be cast into a particularly nice form by exploiting the correspondence between an operator $A : \mathcal{H} \to \mathcal{K}$ and a vector $|A\rangle\rangle$ in $\mathcal{K} \otimes \mathcal{H}$ [7]. Fix orthonormal bases $\{|e_i\rangle\}$ and $\{|e_\mu\rangle\}$ of $\mathcal{H}$ and $\mathcal{K}$, respectively. Then the required correspondence is given by

$$A = \sum_{\mu,i} A_{\mu i} |e_\mu\rangle\langle e_i| \quad \mapsto$$
$$|A\rangle\rangle := \sum_{\mu,i} A_{\mu i} |e_\mu\rangle \otimes |e_i\rangle, \tag{10}$$

so that the double ket $|A\rangle\rangle$ denotes the vector in $\mathcal{K} \otimes \mathcal{H}$ whose components are the matrix elements of A. Let A and B be operators acting on $\mathcal{K}$ and $\mathcal{H}$, respectively, and let C be an operator from $\mathcal{H}$ to $\mathcal{K}$. Then, using Eq. (10), we can readily prove the relations [7]

$$(A \otimes B)|C\rangle\rangle = |ACB^\top\rangle\rangle, \tag{11}$$
$$\mathrm{tr}_2 |A\rangle\rangle\langle\langle B| = AB^*, \tag{12}$$
$$\mathrm{tr}_1 |A\rangle\rangle\langle\langle B| = A^\top \bar{B}, \tag{13}$$

where the subscripts "1" and "2" refer, respectively, to the first and second factors in the tensor product, and $\bar{B}$ is the operator whose matrix elements are complex conjugates of the matrix elements of B. Remarkably, the inner product $\langle\langle A|B\rangle\rangle$ is just the Hilbert–Schmidt

inner product of the operators A and B: $\langle\!\langle A|B\rangle\!\rangle = \mathrm{tr}(A^*B)$.

Using the double-ket notation, we can write $|\varphi_{\mathcal{H}}^+\rangle = |\mathbb{1}\rangle\!\rangle$ with respect to the basis $\{|e_i\rangle\}$. For any set of Kraus operators V_α for the channel T, it can be easily shown that $R_T = \sum_\alpha |V_\alpha\rangle\!\rangle\langle\!\langle V_\alpha|$. It is then an immediate consequence of Eqs. (11) and (12) that

$$
\begin{aligned}
\mathrm{tr}_{\mathcal{H}}\big[\big(\mathbb{1}\otimes\rho^\top\big)R_T\big] &= \sum_\alpha \mathrm{tr}_{\mathcal{H}}\,|V_\alpha\rho\rangle\!\rangle\langle\!\langle V_\alpha| \\
&= \sum_\alpha V_\alpha\rho V_\alpha^*. \tag{14}
\end{aligned}
$$

3. Fidelity for quantum channels and its properties

Let $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$ be a channel. Defining the density operator $\rho_T := (1/d)R_T$, we note that the correspondence $T \mapsto \rho_T$ is obviously one-to-one. Therefore, given two channels $S, T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$, we define the corresponding *fidelity* as

$$
\mathcal{F}(S, T) := F(\rho_S, \rho_T), \tag{15}
$$

where the right-hand side is fidelity (1) between the density operators ρ_S and ρ_T. Properties of the channel fidelity (15) follow directly from the properties of the mixed-state fidelity (1) (see Ref. [1] or [8] for the properties of F and the corresponding proofs), and we now list them with proofs.

Properties of the channel fidelity $\mathcal{F}$

CF1. $0 \leqslant \mathcal{F}(S, T) \leqslant 1$, and $\mathcal{F}(S, T) = 1$ if and only if $S = T$.

CF2. $\mathcal{F}(S, T) = \mathcal{F}(T, S)$ (symmetry).

CF3. For any two unitarily implemented channels $\hat{U}$ and $\hat{V}$ (i.e., $\hat{U}(\rho) = U\rho U^*$ and $\hat{V}(\rho) = V\rho V^*$ with unitary U and V), $\mathcal{F}(\hat{U}, \hat{V}) = (1/d^2)|\,\mathrm{tr}(U^*V)|^2$.

CF4. For any $0 < \lambda < 1$, $\mathcal{F}(S, \lambda T_1 + (1-\lambda)T_2) \geqslant \lambda\mathcal{F}(S, T_1) + (1-\lambda)\mathcal{F}(S, T_2)$ (concavity).

CF5. $\mathcal{F}(S_1 \otimes S_2, T_1 \otimes T_2) = \mathcal{F}(S_1, T_1)\mathcal{F}(S_2, T_2)$ (multiplicativity with respect to tensoring).

CF6. $\mathcal{F}$ is invariant under composition with unitarily implemented channels, i.e., for any unitarily implemented channel $\hat{U}$, $\mathcal{F}(\hat{U} \circ S, \hat{U} \circ T) = \mathcal{F}(S, T)$.

CF7. $\mathcal{F}$ does not decrease under composition with arbitrary channels, i.e., for any channel R, $\mathcal{F}(R \circ S, R \circ T) \geqslant \mathcal{F}(S, T)$.

Proof.

CF1: It follows from the fact that ρ_S and ρ_T are density operators, and from the fact that $T \mapsto \rho_T$ is a one-to-one mapping.

CF2: Same reasoning applies.

CF3: $R_{\hat{U}} = |U\rangle\!\rangle\langle\!\langle U|$, and similarly for $R_{\hat{V}}$. Thus both $\rho_{\hat{U}}$ and $\rho_{\hat{V}}$ are pure states. Since for pure states $|\psi\rangle, |\varphi\rangle$ we have $F = |\langle\psi|\varphi\rangle|^2$, it follows that $\mathcal{F}(\hat{U}, \hat{V}) = (1/d^2)|\langle\!\langle U|V\rangle\!\rangle|^2 = (1/d^2) \times |\,\mathrm{tr}(U^*V)|^2$.

CF4: Note that the map $T \mapsto \rho_T$ is linear. Thus, for $T = \lambda T_1 + (1-\lambda)T_2$, we have $\rho_T = \lambda\rho_{T_1} + (1-\lambda)\rho_{T_2}$, and the concavity of $\mathcal{F}$ follows from the concavity of the mixed-state fidelity (1).

CF5: It follows from Eq. (8) that $\rho_{S\otimes T} = \rho_S \otimes \rho_T$, and the multiplicativity property of $\mathcal{F}$ follows from the corresponding property of F.

CF6: Write $(\hat{U} \circ T) \otimes \mathrm{id} = (\hat{U} \otimes \mathrm{id})(T \otimes \mathrm{id})$ to obtain $\rho_{\hat{U}\circ T} = (U \otimes \mathbb{1})\rho_T(U^* \otimes \mathbb{1})$, and do the same for $\hat{U} \circ S$. Since the mixed-state fidelity F is invariant under unitary transformations, the same property holds for the channel fidelity $\mathcal{F}$.

CF7: Same reasoning as before, except now we have to use the property that $F((R \otimes \mathrm{id})\rho_S, (R \otimes \mathrm{id})\rho_T) \geqslant F(\rho_S, \rho_T)$. $\quad\square$

Despite its fairly obvious definition, the channel fidelity (15) possesses properties that are natural from the physical point of view. First of all, the fact that the channel fidelity is derived from the mixed-state fidelity on a subset of bipartite quantum states implies that, in general, reliable discrimination between quantum channels requires multiparty protocols with entanglement. Indeed, setting $\rho = \rho_S$ and $\sigma = \rho_T$ in the equation [8]

$$
\sqrt{F(\rho, \sigma)} = \min_{\{F_m\}} \sum_m \sqrt{\mathrm{tr}(\rho F_m)\,\mathrm{tr}(\sigma F_m)}, \tag{16}
$$

where the minimum is taken over all positive operator-valued measures (POVMs) $\{F_m\}$, we see that distinguishability of the channels S and T can be related to distinguishability of probability distributions of outcomes of collective measurements on the bipartite system $\mathcal{K} \otimes \mathcal{H}$.

Also, property CF4 implies that mixing channels has adverse effect on distinguishability, and properties CF6 and CF7 show that no *postprocessing*, classical or quantum, can render any two channels more distinguishable. On the other hand, *preprocessing* may improve distinguishability of channels, as we shall see later.

We mention a couple of useful formulas involving $\mathcal{F}$. For instance, the expression for $\mathcal{F}(T, \mathrm{id})$, where T is an arbitrary channel, takes particularly simple form. Let $\{V_\alpha\}$ be any Kraus decomposition of T. Then $\rho_T = (1/d) \sum_\alpha |V_\alpha\rangle\!\rangle\langle\!\langle V_\alpha|$ and, since $\rho_{\mathrm{id}} \equiv (1/d)|\mathbb{1}\rangle\!\rangle\langle\!\langle\mathbb{1}|$ is pure, we have

$$\mathcal{F}(T, \mathrm{id}) = F(\rho_T, \rho_{\mathrm{id}}) = \mathrm{tr}(\rho_{\mathrm{id}}\rho_T)$$
$$= \frac{1}{d^2} \sum_\alpha \big|\langle\!\langle\mathbb{1}|V_\alpha\rangle\!\rangle\big|^2 = \frac{1}{d^2} \sum_\alpha |\mathrm{tr}\, V_\alpha|^2. \quad (17)$$

This implies that, for any two unitarily implemented channels $\hat{U}$ and $\hat{V}$, we have the relation

$$\mathcal{F}(\hat{U}, \hat{V}) = \mathcal{F}(\widehat{U^*V}, \mathrm{id}), \quad (18)$$

where $\widehat{U^*V}$ is the unitarily implemented channel $\rho \mapsto U^*V\rho V^*U$. In other words, distinguishing between two unitarily implemented channels is equivalent to distinguishing between a suitably chosen unitarily implemented channel and the identity channel.

4. Fidelity for quantum channels and Uhlmann's theorem

Our next step is to obtain a meaningful analogue of Uhlmann's theorem for the channel fidelity $\mathcal{F}$. In order to do that, we must draw the connection between the channel T and purifications of the density operator ρ_T.

First let us prove the following: *given a channel* $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$, *where $\mathcal{H}$ and $\mathcal{K}$ are isomorphic Hilbert spaces* ($\mathcal{H} \simeq \mathcal{K}$), *the density operator ρ_T is pure if and only if the channel T is unitarily implemented.* Proving the forward implication is easy: $\rho_{\hat{U}} = (1/d)|U\rangle\!\rangle\langle\!\langle U|$, which is a pure state. Let us now prove the reverse implication. Suppose that, given the channel T, the state ρ_T is pure. As evident from Eq. (7), the reduced density operator $\mathrm{tr}_\mathcal{K}\,\rho_T$ is a multiple of the identity, i.e., it is a maximally mixed state. Since ρ_T is pure, the reduced density operators $\mathrm{tr}_\mathcal{K}\,\rho_T$ and $\mathrm{tr}_\mathcal{H}\,\rho_T$

have the same nonzero eigenvalues [9]. All eigenvalues of $\mathrm{tr}_\mathcal{K}\,\rho_T \equiv (1/d)\mathbb{1}$ are equal and positive. Since $\mathcal{H} \simeq \mathcal{K}$ by assumption, $\mathrm{tr}_\mathcal{K}\,\rho_T$ and $\mathrm{tr}_\mathcal{H}\,\rho_T$ are isospectral. Hence ρ_T is a maximally entangled state and therefore has the form $(1/d)|U\rangle\!\rangle\langle\!\langle U|$ for some unitary U (see the paper by D'Ariano et al. in Ref. [7] for a proof). Using Eq. (11), we can write

$$|U\rangle\!\rangle\langle\!\langle U| = (U \otimes \mathbb{1})|\mathbb{1}\rangle\!\rangle\langle\!\langle\mathbb{1}|(U^* \otimes \mathbb{1}), \quad (19)$$

which implies that $T = \hat{U}$, i.e., T is a unitarily implemented channel.

Therefore, for any two unitarily implemented channels $\hat{U}$ and $\hat{V}$, the states $\rho_{\hat{U}}, \rho_{\hat{V}}$ are already pure and, as we have shown in the previous section,

$$\mathcal{F}(\hat{U}, \hat{V}) = \frac{1}{d^2}\big|\langle\!\langle U|V\rangle\!\rangle\big|^2 \equiv \frac{1}{d^2}\big|\mathrm{tr}(U^*V)\big|^2, \quad (20)$$

which is nothing but the squared normalized Hilbert–Schmidt product of the operators U and V. As we shall now show, the fidelity $\mathcal{F}(S, T)$ for *arbitrary channels* S and T can be expressed as a maximum of expressions similar to the right-hand side of Eq. (20), but with the difference that in place of the unitaries U and V there will appear certain *isometries* from $\mathcal{H}$ to $\mathcal{K} \otimes \mathcal{E}$, where $\mathcal{E}$ is a suitably defined auxiliary Hilbert space.

For this purpose, it is convenient to consider not the channel T, but rather the *dual channel* T_* [10] which converts observables on $\mathcal{K}$ into observables on $\mathcal{H}$, i.e., it is a mapping $T_* : \mathcal{B}(\mathcal{K}) \to \mathcal{B}(\mathcal{H})$, where, e.g., $\mathcal{B}(\mathcal{H})$ is the space of all (bounded) operators on $\mathcal{H}$. The channels T and T_* are related by $\mathrm{tr}(T_*(F)\rho) = \mathrm{tr}(FT(\rho))$, where F is any observable on $\mathcal{K}$ and ρ is any density operator on $\mathcal{H}$. Roughly speaking, the channel T corresponds to the Schrödinger picture of quantum dynamics, while the dual channel T_* describes the Heisenberg picture.

We will need to make use of the Stinespring dilation [10,11] of the dual channel T_*. That is, given T_*, there exist a Hilbert space $\mathcal{E}$ and an isometry $V : \mathcal{H} \to \mathcal{K} \otimes \mathcal{E}$ (i.e., $V^*V = \mathbb{1}_\mathcal{H}$) such that, for any $X \in \mathcal{B}(\mathcal{K})$,

$$T_*(X) = V^*(X \otimes \mathbb{1}_\mathcal{E})V. \quad (21)$$

The isometry V contains complete information about the channel T_* (or, for that matter, T) and is unique up to a unitary transformation of $\mathcal{E}$. In order to arrive at decomposition (21) for T_* from its Kraus representation, fix a set $\{V_\alpha\}_{\alpha=1}^n$ of Kraus operators (it is easy

to see that if $T(\rho)$ is determined from Eq. (3), then $T_*(X) = \sum_\alpha V_\alpha^* X V_\alpha$). Let $\mathcal{E}$ be a Hilbert space of dimension n. We pick an orthonormal basis $\{|e_\alpha\rangle\}_{\alpha=1}^n$ for $\mathcal{E}$ and define the isometry V through its action on an arbitrary vector $|\psi\rangle \in \mathcal{H}$:

$$V|\psi\rangle := \sum_\alpha V_\alpha |\psi\rangle \otimes |e_\alpha\rangle. \tag{22}$$

The action of the adjoint operator V^* on product vectors (elementary tensors) $|\psi\rangle \otimes |\varphi\rangle \in \mathcal{K} \otimes \mathcal{E}$ is given by

$$V^*|\psi\rangle \otimes |\varphi\rangle := \sum_\alpha \langle e_\alpha | \varphi \rangle V_\alpha^* |\psi\rangle, \tag{23}$$

and then extended to all of $\mathcal{K} \otimes \mathcal{E}$ by linearity. The fact that V is an isometry can be easily verified; it is also straightforward to confirm Eq. (21).

Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces with $d = \dim \mathcal{H}$ and $d' = \dim \mathcal{K}$. Our goal is to compute the fidelity $\mathcal{F}(S, T)$ for channels $S, T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$ by "comparing" various Stinespring dilations of their dual channels. In order to do that, we will relate purifications of ρ_S and ρ_T to suitable Stinespring dilations of S_* and T_*, respectively, and then invoke Uhlmann's theorem for the mixed-state fidelity [1,2].

Since ρ_T is a density operator, it possesses a spectral decomposition

$$\rho_T = \sum_{\alpha=1}^{dd'} v_\alpha |\tilde{V}_\alpha\rangle\!\rangle\!\langle\!\langle \tilde{V}_\alpha|, \tag{24}$$

where $\langle\!\langle \tilde{V}_\alpha | \tilde{V}_\beta \rangle\!\rangle = \mathrm{tr}(\tilde{V}_\alpha^* \tilde{V}_\beta) = \delta_{\alpha\beta}$. The operators $V_\alpha := \sqrt{d v_\alpha} \tilde{V}_\alpha$ are then the Kraus operators of T (those V_α that correspond to the zero eigenvalues of ρ_T do not enter into the description of the channel T at all). The purifications of ρ_T can thus be constructed in a $(dd')^2$-dimensional Hilbert space. For instance, the state

$$|\varphi_T\rangle := \sum_{\alpha=1}^{dd'} \sqrt{v_\alpha} |\tilde{V}_\alpha\rangle\!\rangle \otimes |e_\alpha\rangle$$
$$= \frac{1}{\sqrt{d}} \sum_{\alpha=1}^{dd'} |V_\alpha\rangle\!\rangle \otimes |e_\alpha\rangle, \tag{25}$$

where $\{|e_\alpha\rangle\}_{\alpha=1}^{dd'}$ is an orthonormal basis of $\mathcal{E} \simeq \mathcal{K} \otimes \mathcal{H}$, is a purification of ρ_T in the Hilbert space $\mathcal{E}^{\otimes 2}$. It is quite easy to see that

$$|\varphi_T\rangle = \frac{1}{\sqrt{d}} V_{\mathrm{ext}} |\mathbb{1}\rangle\!\rangle, \tag{26}$$

where $V_{\mathrm{ext}} : \mathcal{H}^{\otimes 2} \to \mathcal{K} \otimes \mathcal{H} \otimes \mathcal{E}$ is an isometry defined, for an arbitrary $|\psi\rangle \in \mathcal{H}^{\otimes 2}$, by

$$V_{\mathrm{ext}} |\psi\rangle := \sum_{\alpha=1}^{dd'} \left(V_\alpha \otimes \mathbb{1} |\psi\rangle \right) \otimes |e_\alpha\rangle. \tag{27}$$

The same thing can be carried out for ρ_S. Upon defining the purification

$$|\varphi_S\rangle := \frac{1}{\sqrt{d}} \sum_{\alpha=1}^{dd'} |W_\alpha\rangle\!\rangle \otimes |f_\alpha\rangle \tag{28}$$

of ρ_S (where W_α are Kraus operators for S), the derivation of $|\varphi_S\rangle = (1/\sqrt{d}) W_{\mathrm{ext}} |\mathbb{1}\rangle\!\rangle$ proceeds along the same lines.

Now, according to Uhlmann's theorem [1,2],

$$F(\rho_S, \rho_T) = \max_{|\varphi_S\rangle, |\varphi_T\rangle} \left| \langle \varphi_S | \varphi_T \rangle \right|^2. \tag{29}$$

As evident from the discussion above, any purification of ρ_T can be written in the form $(1/\sqrt{d}) V_{\mathrm{ext}} |\mathbb{1}\rangle\!\rangle$, where the isometry V_{ext} is determined by the eigenvectors $|\tilde{V}_\alpha\rangle\!\rangle$ of ρ_T (or by their images under any unitary transformation of $\mathcal{K} \otimes \mathcal{H}$) and by the choice of basis $\{|e_\alpha\rangle\}$ of $\mathcal{E}$. The same goes for ρ_S, and we can therefore write

$$F(\rho_S, \rho_T) = \frac{1}{d^2} \max_{V_{\mathrm{ext}}, W_{\mathrm{ext}}} \left| \langle\!\langle \mathbb{1} | \left(V_{\mathrm{ext}}^* W_{\mathrm{ext}} \right) \mathbb{1} \rangle\!\rangle \right|^2. \tag{30}$$

It is then an easy exercise to show that

$$\langle\!\langle \mathbb{1} | \left(V_{\mathrm{ext}}^* W_{\mathrm{ext}} \right) \mathbb{1} \rangle\!\rangle = \mathrm{tr}(V^* W), \tag{31}$$

where V and W are isometries $\mathcal{H} \to \mathcal{K} \otimes \mathcal{E}$ that define Stinespring dilations of T and S, respectively, using the same Kraus operators V_α, W_α and the same bases $\{|e_\alpha\rangle\}, \{|f_\alpha\rangle\}$ that appear in the corresponding expressions for V_{ext} and W_{ext}. We thus arrive at the formula

$$\mathcal{F}(S, T) = \frac{1}{d^2} \max_{V, W} \left| \mathrm{tr}(V^* W) \right|^2, \tag{32}$$

which can be taken as the statement of *Uhlmann's theorem for the channel fidelity $\mathcal{F}$*.

5. Applications

Now that we have defined a fidelity measure for quantum channels, and formulated and proved an analogue of Uhlmann's theorem for it, it is time to ask:

can this measure be at all useful? In this section, we offer some examples which suggest that the answer to the above question is "yes".

5.1. Distinguishing channels by superdense coding

It has by now become conventional wisdom in quantum information theory that "you cannot extract more than one bit of classical information out of one qubit" (this assertion can be proved rigorously [12]). In other words, there is no measurement that would allow reliable discrimination between symbols from an alphabet of size $M > 2$ if the corresponding message (of $\log M$ bits) is "carried" by a two-state quantum-mechanical system. However, it is possible for one party to send a 2-bit message to another using a shared entangled state of two qubits in a "superdense coding scheme" [13] (this scheme can in fact be extended [14] to permit reliable discrimination between d^2 symbols with the use of entangled states on a tensor product of two d-dimensional Hilbert spaces).

As noted by Childs et al. [4], the same strategy can be used to improve distinguishability of quantum channels in the following way. Suppose we want to distinguish between d^2 (possibly time-dependent) Hamiltonians H_m, $m \in \{1, \ldots, d^2\}$, acting on a d-dimensional Hilbert space $\mathcal{H}$. We prepare the maximally entangled state $(1/\sqrt{d})|\varphi_{\mathcal{H}}^+\rangle$ and then compare the states

$$|\Psi_m\rangle := \frac{1}{\sqrt{d}}\big(e^{-iH_m t/\hbar} \otimes \mathbb{1}\big)|\varphi_{\mathcal{H}}^+\rangle, \quad m = 1, \ldots, d^2. \tag{33}$$

The idea is to "stop" the entangled state from evolving at such a time t_0 that the quantity $\max_{m \neq n} |\langle\Psi_m|\Psi_n\rangle|^2$ ($m, n = 1, \ldots, d^2$) is minimized (i.e., the pure states $|\Psi_m\rangle \in \mathcal{H}^{\otimes 2}$ are maximally distinguishable).

We can cast this problem into an equivalent form involving the fidelity measure $\mathcal{F}$. We note first that, for each m, the projector $|\Psi_m\rangle\langle\Psi_m|$ is nothing but the state $\rho_{\hat{U}_m}$ for the unitarily implemented channel $\hat{U}_m$ with $U_m := e^{-iH_m t/\hbar}$. That is, $\rho_{\hat{U}_m} = (1/d)|e^{-iH_m t/\hbar}\rangle\!\rangle \langle\!\langle e^{-iH_m t/\hbar}|$ and

$$\big|\langle\Psi_m|\Psi_n\rangle\big|^2 = \frac{1}{d^2}\big|\mathrm{tr}\, e^{-i(H_m - H_n)t/\hbar}\big|^2$$
$$\equiv \mathcal{F}\big(\hat{U}_m, \hat{U}_n\big). \tag{34}$$

If we are to distinguish between the Hamiltonians H_m in fixed time, we are faced with the optimization problem

$$\mathcal{F}_{\mathrm{opt}} = \inf_{t \in [0,T]} \max_{\substack{m,n \in \{1,\ldots,d^2\} \\ m \neq n}} \mathcal{F}\big(\hat{U}_m, \hat{U}_n\big), \tag{35}$$

where T is finite. Provided that the Hamiltonians $H_m(t)$ are sufficiently well-behaved (so that the exponentials e^{-itH_m} are continuous), the maximum of $\mathcal{F}(\hat{U}_m, \hat{U}_n)$ over all pairs (m, n) with m, n distinct is a lower semicontinuous function, and thus attains its infimum on the compact set $[0, T]$.

This problem can be formulated analogously for arbitrary channels T_m, where time dependence can be either continuous (say, via time-dependent Kraus operators) or discrete (e.g., when the channels T_m act on a comparable timescale τ, and we can make measurements only at times $n\tau$, where $n = 0, 1, 2, \ldots$).

5.2. Distinguishing channels with preprocessing

As we have shown earlier, for any three channels R, S, T (where $S, T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$ and $R : \mathcal{S}(\mathcal{K}) \to \mathcal{S}(\mathcal{K}')$, and $\mathcal{H}, \mathcal{K}, \mathcal{K}'$ are Hilbert spaces), we have $\mathcal{F}(R \circ S, R \circ T) \geqslant \mathcal{F}(S, T)$. In other words, when one aims to distinguish between the channels S and T, any postprocessing can only make things worse.

It is pertinent to ask: what about *preprocessing*? Given a pair of channels $S, T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$, can we find a Hilbert space $\mathcal{K}'$ and a channel $R : \mathcal{S}(\mathcal{K}') \to \mathcal{S}(\mathcal{H})$ such that

$$\mathcal{F}(S \circ R, T \circ R) \leqslant \mathcal{F}(S, T)? \tag{36}$$

It turns out that in some cases the answer is "yes". In a recent paper [15], Acín demonstrated the following remarkable fact. Suppose that we have a black box that implements one of two unitaries $U_1, U_2 \in \mathrm{SU}(2)$. In order to tell what the black box does (or, equivalently, to distinguish between these unitaries), the optimal strategy consists of preparing the maximally entangled state $(1/\sqrt{2})(|00\rangle + |11\rangle)$ (here we use the "computational basis" notation so that, e.g., $|00\rangle := |0\rangle \otimes |0\rangle$) and then comparing the states obtained from it by application of the channels $\hat{U}_1 \otimes \mathrm{id}$ and $\hat{U}_2 \otimes \mathrm{id}$. In this case, the measure of distinguishability between U_1 and U_2 (or between the corresponding channels) is given by $\mathcal{F}(\hat{U}_1, \hat{U}_2)$.

Now suppose that we have N copies of the black box and can run them in parallel. If we attempt to compare $U_1^{\otimes N}$ and $U_2^{\otimes N}$ on the basis of the fidelity measure $\mathcal{F}$ alone, we see that $\mathcal{F}_N := \mathcal{F}(\hat{U}_1^{\otimes N}, \hat{U}_2^{\otimes N}) = \mathcal{F}(\hat{U}_1, \hat{U}_2)^N$ (cf. property CF5 of the channel fidelity). If $0 < \mathcal{F}(\hat{U}_1, \hat{U}_2) < 1$, then the fidelity $\mathcal{F}_N$ will decrease exponentially with N, but it will reach zero only in the limit $N \to \infty$. However, as Acín showed in a straightforward argument [15], there exist an integer N_0 and a state $|\Psi\rangle \in \mathcal{H}^{\otimes N_0}$, where $\mathcal{H}$ is a single-qubit Hilbert space, such that $\langle\Psi|(U_1^* U_2)^{\otimes N_0}\Psi\rangle \equiv 0$. This means that the N_0-fold tensor product of the channel $\hat{U}_1$ can be distinguished from the N_0-fold tensor product of the channel $\hat{U}_2$ *perfectly*!

We can express this result in terms of the preprocessing channel T_Ψ that acts on $\mathcal{S}(\mathcal{H}^{\otimes N_0})$ by mapping an arbitrary density operator ρ to the projector $|\Psi\rangle\langle\Psi|$ (i.e., the channel T_Ψ describes the act of preparing the state $|\Psi\rangle$). Thus, for any channel T on $\mathcal{S}(\mathcal{H}^{\otimes N})$,

$$\rho_T = \frac{1}{2^N}(T_{\text{odd}} \otimes \text{id}_{\text{even}})\big(|\varphi_{\mathcal{H}}^+\rangle\langle\varphi_{\mathcal{H}}^+|\big)^{\otimes N},$$

and the channel fidelity $\mathcal{F}(S, T)$ is defined, as before, as the mixed-state fidelity $F(\rho_S, \rho_T)$. Therefore we obtain the result

$$\mathcal{F}(\hat{U}_1, \hat{U}_2) > \mathcal{F}(\hat{U}_1^{\otimes N}, \hat{U}_2^{\otimes N})$$
$$> \mathcal{F}(\hat{U}_1^{\otimes N_0} \circ T_\Psi, \hat{U}_2^{\otimes N_0} \circ T_\Psi) \equiv 0. \quad (37)$$

It certainly is an interesting and important problem to decide whether (and when) preprocessing can improve distinguishability of arbitrary channels. For this purpose, it suffices to consider only *local* preprocessing since, as shown in the paper by D'Ariano et al. in Ref. [7], the action of an arbitrary channel on the maximally entangled state $|\mathbb{1}\rangle\!\rangle\langle\!\langle\mathbb{1}|$ can be represented as the action of a channel of the form $T \otimes \text{id}$. Preprocessing could also involve tensoring S and T with some suitably chosen channel R, but we can exclude such "catalyst" channels because $\mathcal{F}$ is multiplicative with respect to tensor products. Even with these simplifications, however, the preprocessing problem is still quite challenging. A first natural step would be to demonstrate equivalence of $\mathcal{F}$ to some other measure of "distance" between quantum channels. One such measure is induced by the *norm of complete boundedness* (or cb-norm) [10,16] $\|\cdot\|_{\text{cb}}$. That is, $\|S - T\|_{\text{cb}}$

serves as a measure of "closeness" between the channels S and T. For any channel T, $\|T\|_{\text{cb}} = 1$, and $\|S \otimes T\|_{\text{cb}} = \|S\|_{\text{cb}}\|T\|_{\text{cb}}$. Using properties of the cb-norm [10,16], as well as the inequality [3]

$$2 - 2\sqrt{F(\rho, \sigma)} \leqslant \|\rho - \sigma\|_1 \leqslant 2\sqrt{1 - F(\rho, \sigma)},$$

where $\|\cdot\|_1$ is the trace norm [17], it is easy to prove that

$$2 - 2\sqrt{\mathcal{F}(S, T)} \leqslant \|S - T\|_{\text{cb}}. \quad (38)$$

The cb-norm distinguishability measure, however, cannot be used to decide the preprocessing problem for $\mathcal{F}$ since $\|S \circ R - T \circ R\|_{\text{cb}} \leqslant \|S - T\|_{\text{cb}}$, so that, as far as the cb-norm criterion is concerned, any pre- or postprocessing can only make channels less distinguishable. The reason for this is likely to be the following. For any map X between operator algebras, the cb-norm is defined as the supremum, over all positive integers n, of the usual operator norm $\|X \otimes \text{id}_n\|$, where id_n is the identity map on $n \times n$ complex matrices. Thus the cb-norm is a much stronger measure of distinguishability than the channel fidelity $\mathcal{F}$ because preprocessing (at least in terms of initial-state preparation) is implicitly contained in its definition. It is therefore important to determine whether a tight upper bound on $\|S - T\|_{\text{cb}}$ in terms of $\mathcal{F}(S, T)$ can at all be obtained. Inequality (38), on the other hand, can be useful for deriving tight lower bounds on channel capacity.

5.3. Quantum error-correcting codes

Our final example involves the problem of characterizing the performance of a quantum error-correcting code (QECC). We briefly recall the basics of QECCs [18]. The state of a system in a k-dimensional Hilbert space $\mathcal{H}$ is protected by isometrically embedding $\mathcal{H}$ as a k-dimensional subspace $\mathcal{K}$ (the *code*) of an n-dimensional Hilbert space $\mathcal{H}_c$ (the *coding space*). Let the effect of errors be modelled by a channel $T : \mathcal{S}(\mathcal{H}_c) \to \mathcal{S}(\mathcal{H}_c)$. Then, according to a theorem of Knill and Laflamme [18], the subspace $\mathcal{K}$ of $\mathcal{H}_c$ can serve as a QECC for T if and only if there exists a channel $R : \mathcal{S}(\mathcal{H}_c) \to \mathcal{S}(\mathcal{H}_c)$, such that $R \circ T|_{\mathcal{K}} = \text{id}$, where $T|_{\mathcal{K}}$ is the restriction of T to $\mathcal{S}(\mathcal{K})$. The channel R is called the *recovery channel*.

Let $\{|e_i\rangle\}$ be an orthonormal basis of $\mathcal{K}$, and define the corresponding state $|\varphi_{\mathcal{K}}^+\rangle$. Then the above

necessary and sufficient condition is equivalent [18] to the requirement that $(R \circ T)(|\varphi_{\mathcal{K}}^{+}\rangle\langle\varphi_{\mathcal{K}}^{+}|) = |\varphi_{\mathcal{K}}^{+}\rangle\langle\varphi_{\mathcal{K}}^{+}|$. In other words, $\mathcal{K}$ is a T-correcting code if and only if $\mathcal{F}(R \circ T|_{\mathcal{K}}, \mathrm{id}) = 1$.

For the special case of comparing a channel T with the identity channel, we can derive upper and lower bounds on $\mathcal{F}(T, \mathrm{id})$ in terms of $\|T - \mathrm{id}\|_{\mathrm{cb}}$. For this purpose we need the *off-diagonal fidelity* of the channel $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$, defined by [10]

$$\mathcal{F}_{\%}(T) := \sup_{|\psi\rangle, |\varphi\rangle \in \mathcal{H}} \mathrm{Re}\langle\varphi|T(|\varphi\rangle\langle\psi|)\psi\rangle, \tag{39}$$

for which we have the inequality [10]

$$\|T - \mathrm{id}\|_{\mathrm{cb}} \leqslant 4\sqrt{1 - \mathcal{F}_{\%}(T)}. \tag{40}$$

Then $\mathcal{F}(T, \mathrm{id}) \leqslant \mathcal{F}_{\%}(T \otimes \mathrm{id})$, so that, using the fact that the cb-norm is multiplicative with respect to tensor products, we get

$$\|T - \mathrm{id}\|_{\mathrm{cb}} \leqslant 4\sqrt{1 - \mathcal{F}(T, \mathrm{id})}. \tag{41}$$

Combining inequalities (38) and (41) yields

$$\left(1 - \frac{1}{2}\|T - \mathrm{id}\|_{\mathrm{cb}}\right)^{2} \leqslant \mathcal{F}(T, \mathrm{id})$$
$$\leqslant 1 - \frac{1}{16}\|T - \mathrm{id}\|_{\mathrm{cb}}^{2}. \tag{42}$$

The upper bound in this inequality is not nearly as tight as the lower bound. Indeed, when $\|T - \mathrm{id}\|_{\mathrm{cb}}$ equals its maximum value of 2, the fidelity $\mathcal{F}(T, \mathrm{id})$ can take any value between 0 and 3/4. This serves as yet another indication that the cb-norm is a much more stringent distinguishability criterion than the channel fidelity $\mathcal{F}$.

6. Conclusion

In this Letter, we have proposed a fidelity measure $\mathcal{F}$ for quantum channels. This fidelity measure possesses properties that are similar to the properties of the mixed-state fidelity F. We have stated and proved an analogue of Uhlmann's theorem for $\mathcal{F}$ and discussed possible applications of this fidelity measure to problems in quantum information science. We have also outlined the way $\mathcal{F}$ is related to another criterion of channel distinguishability, the cb-norm distance.

References

[1] R. Jozsa, J. Mod. Opt. 41 (1994) 2315.
[2] A. Uhlmann, Rep. Math. Phys. 9 (1976) 273.
[3] C.A. Fuchs, J. van de Graaf, IEEE Trans. Inform. Theory 45 (1999) 1216.
[4] A.M. Childs, J. Preskill, J. Renes, J. Mod. Opt. 47 (2000) 155.
[5] G.M. D'Ariano, P. Lo Presti, Phys. Rev. A 64 (2001) 042308.
[6] J.I. Cirac, W. Dür, B. Kraus, M. Lewenstein, Phys. Rev. Lett. 86 (2001) 544;
P. Zanardi, Phys. Rev. A 63 (2001) R040304.
[7] A. Royer, Phys. Rev. A 43 (1991) 44;
G.M. D'Ariano, P. Lo Presti, M.F. Sacchi, Phys. Lett. A 272 (2000) 32.
[8] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000, Chapter 9.
[9] G. Lindblad, in: Quantum Aspects of Optical Communications, Lecture Notes in Physics, Vol. 378, Springer, 1991, p. 71.
[10] R.F. Werner, in: Quantum Information—an Introduction to Basic Theoretical Concepts and Experiments, Springer Tracts in Modern Physics, Vol. 173, Springer, 2001.
[11] W.F. Stinespring, Proc. Amer. Math. Soc. 6 (1955) 211.
[12] H.P. Yuen, M. Ozawa, Phys. Rev. Lett. 70 (1993) 363.
[13] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[14] R.F. Werner, quant-ph/0003070.
[15] A. Acín, quant-ph/0102064.
[16] A.S. Holevo, R.F. Werner, Phys. Rev. A 63 (2001) 032312.
[17] For any pair ρ, σ of density operators, the trace norm $\|\rho - \sigma\|_{1}$ is twice the trace distance between ρ and σ defined in Ref. [8].
[18] E. Knill, R. Laflamme, Phys. Rev. A 55 (1997) 900.