QUANTUM GATE FIDELITY IN TERMS OF CHOI MATRICES

NATHANIEL JOHNSTON AND DAVID W. KRIBS

Abstract. We provide new results for computing and comparing the quantum gate fidelity of quantum channels via their Choi matrices. We extend recent work that showed there exist non-dual pairs of quantum channels with equal gate fidelity by providing an explicit characterization of all such channels. We use our characterization to show that when the dimension is 2 (or 3, under slightly stronger hypotheses), the gate fidelity of two channels is equal if and only if their difference equals the difference of some unital map and its dual – a fact that has been shown to be false when the dimension is 4 or larger. We also present a formula for the minimum gate fidelity of a channel in terms of a well-studied norm on a compression of its Choi matrix. As a consequence, several new ways of bounding and approximating the minimum gate fidelity follow, including a simple semidefinite program to compute it for qubit channels.

Keywords: quantum gate fidelity, quantum channel, Choi matrix, symmetric subspace

PACS numbers: 03.67.Hk, 03.67.Lx, 02.10.Yn

1. Introduction

In quantum information theory, many of the most important quantum operations are represented ideally by unitary transformations [1]. Experimentally, however, gates are imperfectly implemented via trace-preserving, completely positive maps (called quantum channels). The hope is that the quantum channel which is implemented is in some sense "close" to the desired unitary channel. One of the most common techniques to measure the distance between quantum channels and unitary channels is via the quantum gate fidelity. The gate fidelity is a function, sending pure states to real numbers, that measures the amount of overlap between the output of the unitary channel and the output of the implemented quantum channel. The goal of the present paper is to characterize the gate fidelity in terms of the Choi matrix [2] of a given channel.

Recent work [3] has investigated under what conditions two different quantum channels can have the same gate fidelity. It was demonstrated in that there exist non-dual pairs of channels with the same gate fidelity in all dimensions $n \geq 4$. We extend this work by providing an easily-testable necessary and sufficient condition that described exactly when two channels have the same gate fidelity. We use our characterization to show that for qubit channels, the only way for two channels to have the same gate fidelity is if their difference is the scaled difference of a unital channel and its dual. This property still holds for channels on a 3-dimensional system as long as the channels are unital, but it fails for higher-dimensional channels.

Our characterization of the gate fidelity is in terms of a compression of the Choi matrix of the channel. In addition to being useful for characterizing equality of the gate fidelity, we show that it can be used to calculate the average and variance of the gate fidelity.

Furthermore, we show that the minimum gate fidelity can be phrased in terms of a certain norm [4, 5] on that operator, which allows us to bound the minimum gate fidelity in a variety of new ways and easily compute it for qubit channels.

The remainder of the paper is organized as follows. In Section 2 we introduce the mathematical basics of quantum channels, the gate fidelity, and the measures based on the gate fidelity that are most frequently used. In Section 3 we present the symmetric subspace, flip operator, and Choi matrices, which are the key ingredients in our characterization of the gate fidelity. Section 4 contains our main result, which characterizes gate fidelity in terms of the channel's Choi matrix, and Section 5 specializes our result to the case when the channel acts on a 2- or 3-dimensional system. We close in Section 6 by exploring how our characterization applies to minimum gate fidelity and we demonstrate how to calculate it for qubit channels.

2. Quantum Channels and Gate Fidelity

Throughout this work, we will denote a (finite-dimensional) complex Hilbert space of dimension n by $\mathcal{H}_n$. The space of linear operators on $\mathcal{H}_n$ will be denoted $\mathcal{L}(\mathcal{H}_n)$. We will use I to denote the identity operator on $\mathcal{H}_n$ and id_n to denote the identity operator on $\mathcal{L}(\mathcal{H}_n)$. It will sometimes be useful to associate $\mathcal{H}_n$ with $\mathbb{C}^n$, and $\mathcal{L}(\mathcal{H}_n)$ with the space of $n \times n$ complex matrices via matrix representations of operators in a given orthonormal basis, so we will do so freely without making special mention of that association.

A *pure quantum state* is represented by a unit vector $|\phi\rangle \in \mathcal{H}_n$. We will denote the standard basis of $\mathcal{H}_n$ by $|0\rangle, |1\rangle, \ldots, |n-1\rangle$. We will frequently work with bipartite Hilbert spaces $\mathcal{H}_n \otimes \mathcal{H}_n$, and we will make use of the shorthand notation $|\phi\psi\rangle := |\phi\rangle \otimes |\psi\rangle \in \mathcal{H}_n \otimes \mathcal{H}_n$. One particularly important bipartite pure state is the *maximally entangled* state $|\psi_+\rangle := \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |jj\rangle$.

Not all quantum states are pure however, and a general *mixed quantum state* is represented by positive-semidefinite operator $\rho \in \mathcal{L}(\mathcal{H}_n)$ with $\mathrm{Tr}(\rho) = 1$, where $\mathrm{Tr}(\cdot)$ denotes the trace. Note that a pure state $|\phi\rangle$ can be represented by the operator $|\phi\rangle\langle\phi|$, where $\langle\phi| := |\phi\rangle^\dagger$ is the dual vector of $|\phi\rangle$. The *fidelity* [6, 7] of two quantum states ρ and σ is defined by

$$\mathcal{F}(\rho, \sigma) := \mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2,$$

which reduces in the case when σ is a pure state to simply $\mathcal{F}(\rho, |\phi\rangle\langle\phi|) = \langle\phi|\rho|\phi\rangle$. The fidelity can be thought of as a measure of how well ρ and σ can be distinguished, and it satisfies $0 \leq \mathcal{F}(\rho, \sigma) \leq 1$ with $\mathcal{F}(\rho, \sigma) = 1$ if and only if $\rho = \sigma$.

A *quantum channel* is a completely positive, trace-preserving linear map $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$. Every quantum channel admits a family of *Kraus operators* [1] $\{E_i\}$ such that $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ for all ρ and $\sum_i E_i^\dagger E_i = I$. Given a channel $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$, its *dual channel* $\mathcal{E}^\dagger : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ is defined via the Hilbert-Schmidt inner product to be the unique map such that $\mathrm{Tr}(\mathcal{E}(X)Y) = \mathrm{Tr}(X\mathcal{E}^\dagger(Y))$ for all $X, Y \in \mathcal{L}(\mathcal{H}_n)$. It is the case that $\mathcal{E}^\dagger$ is completely positive if and only if $\mathcal{E}$ is completely positive, and $\mathcal{E}$ is trace-preserving if and only if $\mathcal{E}^\dagger$ is unital – both of these facts can be seen by noting by cyclicity of the trace

shows that

$$\mathrm{Tr}(\mathcal{E}(X)Y) = \mathrm{Tr}\left(\sum_i E_i X E_i^\dagger Y\right) = \mathrm{Tr}\left(X \sum_i E_i^\dagger Y E_i\right),$$

which implies that if $\{E_i\}$ is a family of Kraus operators for $\mathcal{E}$ then $\{E_i^\dagger\}$ is a family of Kraus operators for $\mathcal{E}^\dagger$.

In the special case when a channel $\mathcal{U}$ satisfies $\mathcal{U}(\rho) = U\rho U^\dagger$ for some unitary operator U, $\mathcal{E}$ is called a *unitary channel*. Unitary channels are exactly the channels that do not introduce mixedness (i.e., decoherence) into states and thus they very often are the types of channels that are meant to be implemented in experimental settings. However, no implementation of a channel is perfect – errors are introduced that cause the channel that is implemented to not actually be unitary. The *gate fidelity* is a tool for comparing how well the implemented quantum channel $\mathcal{E}$ approximates the desired unitary channel $\mathcal{U}$. Gate fidelity is a function defined on pure states as follows:

$$\mathcal{F}_{\mathcal{E},\mathcal{U}}(|\phi\rangle) := \mathcal{F}(\mathcal{E}(|\phi\rangle\langle\phi|), \mathcal{U}(|\phi\rangle\langle\phi|)) = \langle\phi|U^\dagger \mathcal{E}(|\phi\rangle\langle\phi|)U|\phi\rangle.$$

Without loss of generality, we can assume $U = I$ by noting that

$$\langle\phi|U^\dagger \mathcal{E}(|\phi\rangle\langle\phi|)U|\phi\rangle = \langle\phi|(\mathcal{U}^\dagger \circ \mathcal{E})(|\phi\rangle\langle\phi|)|\phi\rangle,$$

so $\mathcal{F}_{\mathcal{E},\mathcal{U}} = \mathcal{F}_{\mathcal{U}^\dagger\circ\mathcal{E},id_n}$. For brevity, we will use the shorthand $\mathcal{F}_{\mathcal{E}} := \mathcal{F}_{\mathcal{E},id_n}$, which can be thought of as measuring how noisy the channel $\mathcal{E}$ is. It will also be useful occasionally to consider the gate fidelity of linear maps that are not actually channels. That is, for *any* linear map $\Lambda : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ we define $\mathcal{F}_\Lambda(|\phi\rangle) = \langle\phi|\Lambda(|\phi\rangle\langle\phi|)|\phi\rangle$.

The two most well-studied distance measures based on the gate fidelity are the *average gate fidelity* $\overline{\mathcal{F}_{\mathcal{E}}}$ [8, 9, 10, 11, 12] and the *minimum gate fidelity* [1, 11]

$$\mathcal{F}_{\mathcal{E}}^{min} = \min_{|\phi\rangle} \mathcal{F}_{\mathcal{E}}(|\phi\rangle), \tag{1}$$

which are obtained by either averaging (via the Fubini-Study measure [13]) or minimizing over all pure states $|\phi\rangle$, respectively. The minimum gate fidelity has the interpretation as the most noise that $\mathcal{E}$ can introduce into a quantum system. It makes sense then that one might want instead to minimize $\mathcal{F}(\mathcal{E}(\rho), \rho)$ over all mixed states ρ. The reason we minimize over pure states is that joint concavity of fidelity implies that minimizing over mixed states ρ gives the exact same quantity $\mathcal{F}_{\mathcal{E}}^{min}$ as minimizing over pure states $|\phi\rangle$ – see [1, Section 9.3] or [11, Section IV.C] for a proof of this fact.

One of the most celebrated results concerning gate fidelity is an explicit formula for the average gate fidelity of a quantum channel in terms of its Kraus operators $\{E_i\}$ [8, 9]:

$$\overline{\mathcal{F}_{\mathcal{E}}} = \frac{n + \sum_i |\mathrm{Tr}(E_i)|^2}{n(n+1)}. \tag{2}$$

Similarly, higher-order moments of the gate fidelity have been computed [14, 15]. However, the minimum gate fidelity seems to be much more difficult to compute – for some partial results and bounds on minimum gate fidelity, see [16, 17]. In Section 6 we will derive a formula for the minimum gate fidelity that will allow us to efficiently compute it for qubit channels and derive new bounds for it in general.

3. Choi Matrices and the Symmetric Subspace

To every linear map $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ there is an associated *Choi matrix*:

$$C_{\mathcal{E}} = (id_n \otimes \mathcal{E})(n|\psi_+\rangle\langle\psi_+|).$$

This identification between linear maps on $\mathcal{L}(\mathcal{H}_n)$ and operators in $\mathcal{L}(\mathcal{H}_n \otimes \mathcal{H}_n)$ is known as the *Choi-Jamiolkowski isomorphism*. A celebrated result of Choi says that $\mathcal{E}$ is completely positive if and only if $C_{\mathcal{E}}$ is positive semidefinite [2]. Similarly, $\mathcal{E}$ is trace-preserving if and only if $\mathrm{Tr}_1(C_{\mathcal{E}}) = I$ and $\mathcal{E}$ is unital (i.e., $\mathcal{E}(I) = I$) if and only if $\mathrm{Tr}_2(C_{\mathcal{E}}) = I$, where Tr_j denotes the partial trace over the jth subsystem.

The *flip operator* $F \in \mathcal{L}(\mathcal{H}_n) \otimes \mathcal{L}(\mathcal{H}_n)$ is the Choi matrix of the transpose map T. Its name comes from the fact that $F|\phi\psi\rangle = |\psi\phi\rangle$ for any $|\phi\rangle, |\psi\rangle \in \mathcal{H}_n$. The *symmetric subspace* $\mathcal{S} \subseteq \mathcal{H}_n \otimes \mathcal{H}_n$ is the subspace spanned by the states of the form $|i\rangle|j\rangle + |j\rangle|i\rangle \in \mathcal{H}_n \otimes \mathcal{H}_n$. The Takagi factorization [18, 19] of complex symmetric matrices (and hence symmetric states) says that $|\phi\rangle \in \mathcal{S}$ if and only if $|\phi\rangle$ has a symmetric Schmidt decomposition: $|\phi\rangle = \sum_{j=1}^n \alpha_j |\phi_j\phi_j\rangle$. We will denote the projection of $\mathcal{H}_n \otimes \mathcal{H}_n$ onto $\mathcal{S}$ by $P_{\mathcal{S}}$. Notice that $P_{\mathcal{S}} = \frac{1}{2}(I + F)$ and that the dimension of $\mathcal{S}$ is $n(n+1)/2$.

We now present a simple proposition concerning the average gate fidelity. While this proposition may not appear particularly useful considering we already have Equation (2) to work with, it gives $\overline{\mathcal{F}_{\mathcal{E}}}$ in terms of the operator $P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$. We will see this operator repeatedly throughout this work, most notably in a characterization of the gate fidelity and also in a formula for the minimum gate fidelity, and hence it is useful to see how it relates to the average gate fidelity as well. Observe that the scaling factor $2/(n(n+1))$ in the following result is exactly one divided by the dimension of $\mathcal{S}$, so average gate fidelity can be seen as an average over the symmetric subspace.

Proposition 1. *Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ be a quantum channel. Then*

$$\overline{\mathcal{F}_{\mathcal{E}}} = \frac{2}{n(n+1)} \mathrm{Tr}\big(P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}\big).$$

Proof. The proof is by straightforward algebra. If we write $C_{\mathcal{E}}$ in its spectral decomposition $\sum_i \lambda_i |v_i\rangle\langle v_i|$, then

$$\begin{aligned}
\mathrm{Tr}\big((T \otimes id_n)(C_{\mathcal{E}})(2P_{\mathcal{S}} - I)\big) &= \mathrm{Tr}\big((T \otimes id_n)(C_{\mathcal{E}})F\big) \\
&= \mathrm{Tr}\big((T \otimes id_n)(C_{\mathcal{E}})(id_n \otimes T)(n|\psi_+\rangle\langle\psi_+|)\big) \\
&= n\langle\psi_+|C_{\mathcal{E}}|\psi_+\rangle \\
&= n\sum_i \lambda_i |\langle\psi_+|v_i\rangle|^2 \\
&= \sum_i |\mathrm{Tr}(E_i)|^2,
\end{aligned}$$

where the third equality follows from the identity $T^\dagger = T$, and the final equality comes from the fact that the (scaled) eigenvectors of $C_{\mathcal{E}}$ are the vectorizations of the Kraus operators of $\mathcal{E}$. The result follows from Equation (2) and the fact that $\mathcal{E}$ is trace-preserving, so $\mathrm{Tr}((T \otimes id_n)(C_{\mathcal{E}})) = n$. □

In fact, the proof of Proposition 1 shows that $(2/n^2)\mathrm{Tr}\big(P_{\mathcal{S}}(T\otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}\big) - 1/n = \langle\psi_+|C_{\mathcal{E}}|\psi_+\rangle/n$, a quantity that was referred to as $\chi_{0,0}$ in [15]. It follows that the formulas for the variance and higher-order moments of $\mathcal{F}_{\mathcal{E}}$ can be written in terms of the operator $P_{\mathcal{S}}(T\otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$ as well.

For completeness, we close this section with a well-known fact that shows how the Choi matrices of a pair of dual channels $\mathcal{E}$ and $\mathcal{E}^\dagger$ are related to each other. For another proof in the more general case of positive (not necessarily completely positive) maps, see [20, Lemma 3].

Lemma 2. *Let $\mathcal{E}:\mathcal{L}(\mathcal{H}_n)\to\mathcal{L}(\mathcal{H}_n)$ be a quantum channel. Then $C_{\mathcal{E}^\dagger} = FC_{\mathcal{E}}^T F$.*

Proof. Use the spectral decomposition to write $C_{\mathcal{E}} = \sum_i \lambda_i |v_i\rangle\langle v_i|$. Then $C_{\mathcal{E}}^T = \sum_i \lambda_i \overline{|v_i\rangle\langle v_i|}$. It is easily verified that for any $X\in\mathcal{L}(\mathcal{H}_n)$, the vectorization of X^T is exactly F times the vectorization of X. The result follows from recalling that $\{E_i\}$ is a set of Kraus operators for $\mathcal{E}$ if and only if $\{E_i^\dagger\}$ is a set of Kraus operators for $\mathcal{E}^\dagger$, and that the Kraus operators of a channel can be chosen so that their vectorizations are the eigenvectors of $C_{\mathcal{E}}$. □

4. Channels with Identical Gate Fidelity

It was shown in [3] that if $n\geq 4$ and $\mathcal{E}:\mathcal{L}(\mathcal{H}_n)\to\mathcal{L}(\mathcal{H}_n)$ is a quantum channel with positive-definite Choi matrix, then there exists another quantum channel $\mathcal{R}:\mathcal{L}(\mathcal{H}_n)\to\mathcal{L}(\mathcal{H}_n)$ with $\mathcal{R}\neq\mathcal{E},\mathcal{E}^\dagger$ such that $\mathcal{F}_{\mathcal{E}} = \mathcal{F}_{\mathcal{R}}$. A particular consequence of this result is the fact that there exist non-depolarizing quantum channels with constant gate fidelity. In this section we expand on this work by providing an easily-testable characterization of when two maps have the same gate fidelity in terms of their Choi matrices.

We begin with a lemma that allows us to talk about $\mathcal{F}_{\mathcal{E}}(|\phi\rangle)$ in terms of the Choi matrix of $\mathcal{E}$. This lemma is in essence a simplification of [3, Lemma 1], but we present it here for completeness, along with a simplified proof.

Lemma 3. *Let $\Lambda:\mathcal{L}(\mathcal{H}_n)\to\mathcal{L}(\mathcal{H}_n)$ be a linear map and let $|\phi\rangle\in\mathcal{H}_n$. Then*

$$\mathcal{F}_\Lambda(|\phi\rangle) = \langle\phi\phi|(T\otimes id_n)(C_\Lambda)|\phi\phi\rangle.$$

Proof. The proof is by simple algebra.

$$\begin{aligned}
\langle\phi\phi|(T\otimes id_n)(C_\Lambda)|\phi\phi\rangle &= \sum_{i,j=0}^{n-1}\langle\phi\phi|(T(|i\rangle\langle j|)\otimes\Lambda(|i\rangle\langle j|))|\phi\phi\rangle\\
&= \sum_{i,j=0}^{n-1}\langle\phi|j\rangle\langle i|\phi\rangle\langle\phi|\Lambda(|i\rangle\langle j|)|\phi\rangle\\
&= \langle\phi|\Lambda\big((\sum_{i=0}^{n-1}\langle i|\phi\rangle|i\rangle)(\sum_{j=0}^{n-1}\langle\phi|j\rangle\langle j|)\big)|\phi\rangle\\
&= \langle\phi|\Lambda(|\phi\rangle\langle\phi|)|\phi\rangle\\
&= \mathcal{F}_\Lambda(|\phi\rangle).
\end{aligned}$$

□

We are now ready to state the main result of this section, which allows us to determine whether or not two quantum channels have the same gate fidelity simply by comparing a certain modification of their Choi matrices. In particular, we see that the gate fidelity of a channel $\mathcal{E}$ is determined exactly by the operator $P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$. Note that the "if" direction of this result follows trivially from [3, Lemma 1], so what is new here is the "only if" direction.

Theorem 4. *Let $Q, R : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ be linear maps. Then $\mathcal{F}_Q = \mathcal{F}_R$ if and only if*

$$P_{\mathcal{S}}(T \otimes id_n)(C_Q)P_{\mathcal{S}} = P_{\mathcal{S}}(T \otimes id_n)(C_R)P_{\mathcal{S}}.$$

Proof. We begin by defining $D := (T \otimes id_n)(C_Q - C_R)$. Using Lemma 3 with $\Lambda := Q - R$ shows that $\mathcal{F}_Q = \mathcal{F}_R$ if and only if

$$\langle \phi\phi | D | \phi\phi \rangle = 0 \quad \forall\, |\phi\rangle \in \mathcal{H}_n. \tag{3}$$

If we can show that Equation (3) implies

$$\langle s_1 | D | s_2 \rangle = 0 \quad \forall\, |s_1\rangle, |s_2\rangle \in \mathcal{S},$$

we will be done. To this end, fix arbitrary $|\phi\rangle, |\psi\rangle \in \mathcal{H}_n$ and let $z \in \mathbb{C}$ be such that $|z| = 1$. Then Equation (3) implies that

$$(\langle\phi| + \overline{z}\langle\psi|) \otimes (\langle\phi| + \overline{z}\langle\psi|)D(|\phi\rangle + z|\psi\rangle) \otimes (|\phi\rangle + z|\psi\rangle) = 0 \quad \text{and} \tag{4}$$

$$(\langle\phi| - \overline{z}\langle\psi|) \otimes (\langle\phi| - \overline{z}\langle\psi|)D(|\phi\rangle - z|\psi\rangle) \otimes (|\phi\rangle - z|\psi\rangle) = 0. \tag{5}$$

If we expand and add Equations (4) and (5) together and use (3), we see that for all $z \in \mathbb{C}$ with $|z| = 1$,

$$z^2\langle\phi\phi|D|\psi\psi\rangle + \overline{z}^2\langle\psi\psi|D|\phi\phi\rangle + (\langle\phi\psi| + \langle\psi\phi|)D(|\phi\psi\rangle + |\psi\phi\rangle) = 0. \tag{6}$$

If we subtract from Equation (6) the equation obtained by replacing z in Equation (6) by iz, we learn that

$$z^2\langle\phi\phi|D|\psi\psi\rangle + \overline{z}^2\langle\psi\psi|D|\phi\phi\rangle = 0 \quad \forall z \in \mathbb{C} \text{ with } |z| = 1.$$

The following two equations arise from letting $z = 1$ and $z = e^{i\pi/4}$, respectively:

$$\langle\phi\phi|D|\psi\psi\rangle + \langle\psi\psi|D|\phi\phi\rangle = 0$$
$$i\langle\phi\phi|D|\psi\psi\rangle - i\langle\psi\psi|D|\phi\phi\rangle = 0.$$

Adding i times the first equation to the second equation gives

$$\langle\phi\phi|D|\psi\psi\rangle = 0 \quad \forall\, |\phi\rangle, |\psi\rangle \in \mathcal{H}_n. \tag{7}$$

Now let $|s_1\rangle, |s_2\rangle \in \mathcal{S}$. By the Takagi factorization we know that we can write $|s_1\rangle = \sum_{j=1}^n \alpha_j |\phi_j\phi_j\rangle$ and $|s_2\rangle = \sum_{k=1}^n \beta_k |\psi_k\psi_k\rangle$. Thus

$$\langle s_1 | D | s_2 \rangle = \sum_{j,k=1}^n \alpha_j\beta_k \langle\phi_j\phi_j|D|\psi_k\psi_k\rangle = 0,$$

since each term in the sum equals zero by Equation (7). This completes the proof. □

As a particularly important special case of Theorem 4, consider the case of channels with constant gate fidelity. It is easily shown that any depolarizing channel has constant gate fidelity, and it was shown in [3] that there exist non-depolarizing channels with constant gate fidelity. We now present a characterization of all channels with constant gate fidelity.

Corollary 5. *Let $Q : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ be a linear map and let $c \in \mathbb{R}$. Then $\mathcal{F}_Q \equiv c$ if and only if $P_{\mathcal{S}}(T \otimes id_n)(C_Q)P_{\mathcal{S}} = cP_{\mathcal{S}}$.*

Proof. Consider the linear map $R : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ defined by $R(X) = \frac{1}{n-1}\big((cn-1)X + (1-c)I\big)$ (if $1/n \leq c \leq 1$ then R is a depolarizing quantum channel). Simple algebra reveals that

$$\mathcal{F}_R(|\phi\rangle) = \frac{1}{n-1}\langle\phi|\big((cn-1)|\phi\rangle\langle\phi| + (1-c)I\big)|\phi\rangle = \frac{(cn-1)+(1-c)}{n-1} = c$$

for any $|\phi\rangle \in \mathcal{H}_n$. Also, $(T \otimes id_n)(C_R) = \frac{1}{n-1}\big((cn-1)F + (1-c)(I \otimes I)\big)$. Thus,

$$P_{\mathcal{S}}(T \otimes id_n)(C_R)P_{\mathcal{S}} = \frac{1}{n-1}\big((cn-1)P_{\mathcal{S}} + (1-c)P_{\mathcal{S}}\big) = cP_{\mathcal{S}}.$$

Using Theorem 4 gives the result. □

Corollary 5 can be seen in terms of the higher-rank numerical range of the operator $(T \otimes id_n)(C_Q)$ [21]. In particular, it implies that if Q has constant gate fidelity, then $(T \otimes id_n)(C_Q)$ must have non-empty rank-$[n(n+1)/2]$ numerical range. Because the higher-rank numerical range of a Hermitian operator is well-understood in terms of its eigenvalues, it follows that the middle n eigenvalues of $(T \otimes id_n)(C_Q)$ must all be equal in order for Q to have constant gate fidelity.

5. Gate Fidelity in Small Dimensions

Note that for any quantum channel $\mathcal{E}$ and state $|\phi\rangle \in \mathcal{H}_n$ it is trivially the case that $\mathrm{Tr}(\mathcal{E}(|\phi\rangle\langle\phi|)|\phi\rangle\langle\phi|) = \mathrm{Tr}(\mathcal{E}^\dagger(|\phi\rangle\langle\phi|)|\phi\rangle\langle\phi|)$, so $\mathcal{F}_{\mathcal{E}} = \mathcal{F}_{\mathcal{E}^\dagger}$. Similarly, if $\mathcal{Q}$ is a quantum channel, $r \geq 0$, and $\mathcal{E}$ is a quantum channel, then $\mathcal{Q} + r(\mathcal{E} - \mathcal{E}^\dagger)$ also has gate fidelity equal to that of $\mathcal{Q}$. A particular consequence of this observation is that for any quantum channel $\mathcal{Q}$ with full-rank Choi matrix, there is another quantum channel (not equal to $\mathcal{Q}^\dagger$) with the same gate fidelity – a fact that was originally proved in dimensions $n \geq 4$ in [3]. To construct such a map it suffices to pick a unital channel $\mathcal{E}$ and then choose a sufficiently small $r > 0$.

A natural question to ask is whether or not the converse of the observation made in the previous paragraph holds. That is, if two quantum channels $\mathcal{Q}$ and $\mathcal{R}$ have the same gate fidelity, do they differ by some $r(\mathcal{E} - \mathcal{E}^\dagger)$? One simplification we can make right away is that we can assume without loss of generality that $\mathcal{E}$ is unital. Indeed, it is easily-verified that the channel $\mathcal{E}$ is unital if and only if $\mathcal{R} = \mathcal{Q} + r(\mathcal{E} - \mathcal{E}^\dagger)$ is trace-preserving. The example used in the construction of [3, Theorem 1] shows that such a channel $\mathcal{E}$ need not exist when $n \geq 4$, even if $\mathcal{Q}, \mathcal{R}$ are assumed to be unital. We now present an example to show that $\mathcal{E}$ need not exist when $n = 3$, as long as we do not require that $\mathcal{Q}$ and $\mathcal{R}$ be unital.

Example 6. Consider the two channels $\mathcal{Q}, \mathcal{R} : \mathcal{L}(\mathcal{H}_3) \to \mathcal{L}(\mathcal{H}_3)$ defined in the standard basis by the following Choi matrices:

$$C_{\mathcal{Q}} := \frac{1}{4}\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}, \quad C_{\mathcal{R}} := \frac{1}{4}\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

It is easily verified that $C_{\mathcal{Q}}$ and $C_{\mathcal{R}}$ are both positive semidefinite and $\mathrm{Tr}_2(C_{\mathcal{Q}}) = \mathrm{Tr}_2(C_{\mathcal{R}}) = I$, so $\mathcal{Q}$ and $\mathcal{R}$ are both indeed quantum channels (but $\mathrm{Tr}_1(C_{\mathcal{Q}}) = I \neq \mathrm{Tr}_1(C_{\mathcal{R}})$ so $\mathcal{Q}$ is unital but $\mathcal{R}$ is not). It is also easily verified that $P_{\mathcal{S}}(T \otimes id_3)(C_{\mathcal{Q}} - C_{\mathcal{R}})P_{\mathcal{S}} = 0$, so $\mathcal{F}_{\mathcal{Q}} = \mathcal{F}_{\mathcal{R}}$ by Theorem 4.

On the other hand, because $\mathcal{Q}$ is unital, it follows that if $\mathcal{E}$ is a unital quantum channel then $\mathcal{Q}(I) + r(\mathcal{E}(I) - \mathcal{E}^\dagger(I)) = I + r(I - I) = I$, so $\mathcal{Q} + r(\mathcal{E} - \mathcal{E}^\dagger)$ is unital as well. Thus there does not exist $r \geq 0$ and a unital quantum channel $\mathcal{E}$ such that $\mathcal{R} = \mathcal{Q} + r(\mathcal{E} - \mathcal{E}^\dagger)$.

We now present the main result of this section, which shows that when $n = 2$, the converse of our previous observation does indeed hold. That is, if two qubit channels have the same gate fidelity then their difference equals the scaled difference of some pair of dual channels. We also show that this converse still holds when $n = 3$, in spite of Example 6, under some slightly stronger hypotheses.

Theorem 7. *Let $\mathcal{Q}, \mathcal{R} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ be quantum channels. Suppose that either $n = 2$, or $n = 3$ and $\mathcal{Q}(I) = \mathcal{R}(I)$. Then $\mathcal{F}_{\mathcal{Q}} = \mathcal{F}_{\mathcal{R}}$ if and only if there exists $r \geq 0$ and a unital quantum channel $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ such that $\mathcal{R} = \mathcal{Q} + r(\mathcal{E} - \mathcal{E}^\dagger)$.*

Proof. As has already been discussed, the "if" direction clearly holds in any dimension. To see the "only if" direction, we first consider the case when $n = 2$. Let's choose an orthogonal basis of (unnormalized) symmetric and antisymmetric states:

$$|a\rangle := |01\rangle - |10\rangle, \quad |s_1\rangle := |01\rangle + |10\rangle, \quad |s_2\rangle := |00\rangle, \quad |s_3\rangle := |11\rangle.$$

From Theorem 4 we know $P_{\mathcal{S}}(T \otimes id_2)(C_{\mathcal{Q}} - C_{\mathcal{R}})P_{\mathcal{S}} = 0$. Thus there exist $\alpha \in \mathbb{R}$ and $c_1, c_2, c_3 \in \mathbb{C}$ such that we can write

$$(T \otimes id_2)(C_{\mathcal{Q}} - C_{\mathcal{R}}) = \alpha |a\rangle\langle a| + \sum_{j=1}^{3} \big(c_j |a\rangle\langle s_j| + \overline{c_j} |s_j\rangle\langle a|\big).$$

The fact that $\mathcal{Q}$ and $\mathcal{R}$ are trace-preserving implies that $\mathrm{Tr}_2(C_{\mathcal{Q}}) = \mathrm{Tr}_2(C_{\mathcal{R}}) = I$, which implies that $\alpha = 0$, c_1 is purely imaginary, and $c_3 = \overline{c_2}$. It follows that we can write

$(T \otimes id_2)(C_{\mathcal{Q}} - C_{\mathcal{R}})$ in the standard basis as

$$(T \otimes id_2)(C_{\mathcal{Q}} - C_{\mathcal{R}}) = \begin{bmatrix} 0 & \overline{c_2} & -\overline{c_2} & 0 \\ c_2 & 0 & 2c_1 & \overline{c_2} \\ -c_2 & 2\overline{c_1} & 0 & -\overline{c_2} \\ 0 & c_2 & -c_2 & 0 \end{bmatrix}. \tag{8}$$

Now choose $r \geq 2|c_2| + 2|c_1|$ and define a channel $\mathcal{E} : \mathcal{L}(\mathcal{H}_2) \to \mathcal{L}(\mathcal{H}_2)$ via the Choi matrix

$$C_{\mathcal{E}} = \frac{1}{2r} \begin{bmatrix} r & 0 & -2c_2 & 2\overline{c_1} \\ 0 & r & 0 & 2c_2 \\ -2\overline{c_2} & 0 & r & 0 \\ 2c_1 & 2\overline{c_2} & 0 & r \end{bmatrix}.$$

It is easily verified that $\mathrm{Tr}_1(C_{\mathcal{E}}) = \mathrm{Tr}_2(C_{\mathcal{E}}) = I$ so $\mathcal{E}$ is unital and trace-preserving, and the fact that $\mathcal{E}$ is completely positive follows from the fact that its Choi matrix is diagonally dominant and hence positive semidefinite. It is a simple calculation using Lemma 2 to verify that

$$r(T \otimes id_2)(C_{\mathcal{E}} - C_{\mathcal{E}^\dagger}) = \begin{bmatrix} 0 & \overline{c_2} & -\overline{c_2} & 0 \\ c_2 & 0 & 2c_1 & \overline{c_2} \\ -c_2 & 2\overline{c_1} & 0 & -\overline{c_2} \\ 0 & c_2 & -c_2 & 0 \end{bmatrix}. \tag{9}$$

By comparing Equations (8) and (9) we see that $\mathcal{Q} - \mathcal{R} = r(\mathcal{E} - \mathcal{E}^\dagger)$, which completes the proof for the case when $n = 2$.

The case when $n = 3$ and $\mathcal{Q}(I) = \mathcal{R}(I)$ is proved analogously, but the algebra is more involved. Choose an orthogonal basis of (unnormalized) symmetric and antisymmetric states:

$$\begin{aligned} |a_1\rangle &:= |01\rangle - |10\rangle, & |s_1\rangle &:= |01\rangle + |10\rangle \\ |a_2\rangle &:= |02\rangle - |20\rangle, & |s_2\rangle &:= |02\rangle + |20\rangle \\ |a_3\rangle &:= |12\rangle - |21\rangle, & |s_3\rangle &:= |12\rangle + |21\rangle \\ & & |s_4\rangle &:= |00\rangle \\ & & |s_5\rangle &:= |11\rangle \\ & & |s_6\rangle &:= |22\rangle \end{aligned}$$

From Theorem 4 we know $P_{\mathcal{S}}(T \otimes id_3)(C_{\mathcal{Q}} - C_{\mathcal{R}})P_{\mathcal{S}} = 0$. Thus there exist $\{\alpha_j\} \in \mathbb{R}$ and $\{c_{j,k}\} \in \mathbb{C}$ $(1 \leq j \leq 3, 1 \leq k \leq 6)$ such that we can write

$$(T \otimes id_3)(C_{\mathcal{Q}} - C_{\mathcal{R}}) = \sum_{j=1}^{3} \alpha_j |a_j\rangle\langle a_j| + \sum_{j=1}^{3} \sum_{k=1}^{6} \left(c_{j,k} |a_j\rangle\langle s_k| + \overline{c_{j,k}} |s_k\rangle\langle a_j| \right).$$

The facts that $\mathcal{Q}$ and $\mathcal{R}$ are trace-preserving and $\mathcal{Q}(I) = \mathcal{R}(I)$ imply that $\mathrm{Tr}_1((T \otimes id_3)(C_{\mathcal{Q}} - C_{\mathcal{R}})) = \mathrm{Tr}_2((T \otimes id_3)(C_{\mathcal{Q}} - C_{\mathcal{R}})) = 0$, which implies $\alpha_1 = \alpha_2 = \alpha_3 = 0$. The partial trace

conditions also imply the following conditions:

$$\begin{aligned}\mathrm{Re}(c_{1,1}) = \mathrm{Re}(c_{3,3}) &= -\mathrm{Re}(c_{2,2}) \\ c_{2,3} &= \overline{c_{1,4}} - c_{1,5} - \overline{c_{3,2}} \\ c_{2,6} &= \overline{c_{2,4}} + \overline{c_{3,1}} - c_{1,3} \\ c_{3,6} &= c_{1,2} + \overline{c_{2,1}} + \overline{c_{3,5}}\end{aligned}$$

If $c_{1,1} = b + id_1$, $\mathrm{Im}(c_{2,2}) = d_2$ and $\mathrm{Im}(c_{3,3}) = d_3$ then we can write $(T \otimes id_3)(C_{\mathcal{Q}} - C_{\mathcal{R}})$ in the standard basis as

(10)
$$\begin{bmatrix}
0 & \overline{c_{1,4}} & \overline{c_{2,4}} & -\overline{c_{1,4}} & 0 & \overline{c_{3,4}} & -\overline{c_{2,4}} & -\overline{c_{3,4}} & 0 \\
* & 2b & c_{1,2} + \overline{c_{2,1}} & 2id_1 & c_{1,5} & c_{1,3} + \overline{c_{3,1}} & c_{1,2} - \overline{c_{2,1}} & c_{1,3} - \overline{c_{3,1}} & c_{1,6} \\
* & * & -2b & -\overline{c_{1,2}} + c_{2,1} & c_{2,5} & \overline{c_{1,4}} - c_{1,5} & 2id_2 & c_{2,3} - \overline{c_{3,2}} & c_{2,6} \\
* & * & * & -2b & -c_{1,5} & \overline{c_{3,1}} - c_{1,3} & -\overline{c_{2,1}} - c_{1,2} & -\overline{c_{3,1}} - c_{1,3} & -c_{1,6} \\
* & * & * & * & 0 & \overline{c_{3,5}} & -\overline{c_{2,5}} & -\overline{c_{3,5}} & 0 \\
* & * & * & * & * & 2b & c_{3,2} - \overline{c_{2,3}} & 2id_3 & c_{3,6} \\
* & * & * & * & * & * & 2b & -\overline{c_{1,4}} + c_{1,5} & -c_{2,6} \\
* & * & * & * & * & * & * & -2b & -c_{3,6} \\
* & * & * & * & * & * & * & * & 0
\end{bmatrix},$$

where the $*$ in the (j,k)-entry indicates the complex conjugate of the (k,j)-entry. Now let $r > 0$ be arbitrarily large, $\varepsilon > 0$ and $0 < s, t < 1 - \varepsilon$, and define $u := 1 - \varepsilon - s$ and $v := 1 - \varepsilon - t$. We shall consider the linear map $\mathcal{E}$ defined by the Choi matrix

$$C_{\mathcal{E}} = \frac{1}{3r}\begin{bmatrix}
3r\varepsilon & 0 & 0 & -3c_{1,4} & -3id_1 & -3c_{1,2} & -3c_{2,4} & -3c_{2,1} & -3id_2 \\
* & 3rs & 3c_{1,2} & 0 & 0 & 0 & -3c_{3,4} & -3c_{3,1} & 3c_{1,4} - 6c_{3,2} \\
* & * & 3ru & 0 & 3\overline{c_{1,3}} & 3c_{1,4} & 0 & 0 & 3c_{2,4} + 3c_{3,1} \\
* & * & * & 3rt & -3c_{1,5} & -3c_{1,3} & -3c_{2,1} & -3c_{2,5} & 3c_{1,5} \\
* & * & * & * & 3r\varepsilon & 0 & -3c_{3,1} & -3c_{3,5} & -3id_3 \\
* & * & * & * & * & 3rv & -3\overline{c_{1,6}} & 0 & 3c_{2,1} + 3c_{3,5} \\
* & * & * & * & * & * & 3rv & 3c_{1,5} & 3c_{1,3} \\
* & * & * & * & * & * & * & 3ru & -3c_{1,2} \\
* & * & * & * & * & * & * & * & 3r(1-u-v)
\end{bmatrix}.$$

In particular, choose s and t so that $s+t \geq 1$ and $s-t = 2b/r$. This is always possible because we can choose s so that $2b/r < s < 1$, set $t = s - 2b/r$, and then choose some sufficiently small $\varepsilon > 0$. It follows that each diagonal entry of $C_{\mathcal{E}}$ is strictly positive, and so by choosing r sufficiently large it becomes diagonally dominant and hence positive semidefinite. It is worth noting that, although t does depend on r, increasing r only increases t so diagonal dominance won't be interfered with as t varies. It is easily verified that $\mathrm{Tr}_1(C_{\mathcal{E}}) = \mathrm{Tr}_2(C_{\mathcal{E}}) = I$ so $\mathcal{E}$ is in fact a unital quantum channel.

Furthermore, it is a simple (albeit tedious) calculation using Lemma 2 to verify that $r(T \otimes id_2)(C_{\mathcal{E}} - C_{\mathcal{E}^\dagger})$, when written in the standard basis, is exactly the matrix (10). It follows that $\mathcal{Q} - \mathcal{R} = r(\mathcal{E} - \mathcal{E}^\dagger)$, which completes the proof. □

It is worth pointing out where the techniques used in the proof of Theorem 7 break down in the $n \geq 4$ case. The proofs in the $n = 2$ and $n = 3$ cases both begin by making use of the

constraint $\mathrm{Tr}_2((T \otimes id_n)(C_{\mathcal{Q}} - C_{\mathcal{R}})) = 0$ (and similarly for Tr_1 when $n = 3$) to restrict the $n(n-1)/2$ real and $n^2(n-1)(n+1)/4$ complex coefficients that define $(T \otimes id_n)(C_{\mathcal{Q}} - C_{\mathcal{R}})$. In particular, we need the partial trace restrictions to imply that $P_{\mathcal{A}}(T \otimes id_n)(C_{\mathcal{Q}} - C_{\mathcal{R}})P_{\mathcal{A}} = 0$, where $P_{\mathcal{A}} := I - P_{\mathcal{S}}$ is the projection onto the antisymmetric subspace. In the $n \geq 4$ case the two partial trace constraints aren't strong enough to guarantee this property holds, as demonstrated by the map in the proof of [3, Theorem 1].

6. Minimum Gate Fidelity

Calculating the minimum gate fidelity is a problem that is expected to be difficult, and few general methods of approximating and bounding it are known. Our main result of this section shows that the minimal fidelity of a channel can be written in terms of the $S(1)$-norm [4, 5], defined on positive semidefinite operators as

$$\big\|X\big\|_{S(1)} := \sup_{|\phi\rangle, |\psi\rangle} \big\{\langle\phi\psi|X|\phi\psi\rangle\big\}.$$

Our reason for expressing the minimum gate fidelity in terms of this norm rather than in terms of other related minimizations or maximizations is that several bounds, inequalities and properties of the $S(1)$-norm are already known [4, 5, 22, 23], whereas other similar supremums or infimums appear to be more nebulous. In particular, computation of the $S(1)$-norm on positive semidefinite operators is equivalent to the problem of determining whether or not a given operator is an entanglement witness [4, Corollary 4.9], which is equivalent to the problem of determining whether or not a superoperator is positive. The problems of characterizing positive superoperators [24, 25] and entanglement witnesses and separable states [26, 27, 28, 29, 30, 31] have been studied extensively, so an abundance of results from operator theory and entanglement theory now apply in this setting.

All separability criteria that have been developed over the past several years now automatically translate into methods of bounding minimum gate fidelity. As a particularly important example of this, symmetric extensions [29] can now be used to compute minimum gate fidelity within any desired accuracy simply by performing the optimization over separable states over the set of states with k-symmetric extension instead. The optimization over states with k-symmetric extension is a semidefinite program [32], which can be computed efficiently [33], and precise bounds for how far away the optimal value of the kth semidefinite program is from the optimization over separable states are given in [34].

Theorem 8. *Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ be a quantum channel and let λ_1 be the maximal eigenvalue of $P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$. Then*

$$\mathcal{F}_{\mathcal{E}}^{min} = \lambda_1 - \big\|\lambda_1 P_{\mathcal{S}} - P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}\big\|_{S(1)}.$$

Proof. Using Lemma 3 with $\Lambda := \mathcal{E}$ reveals that

$$\mathcal{F}_{\mathcal{E}}^{min} = \min_{|\phi\rangle \in \mathcal{H}_n} \big\{\langle\phi\phi|(T \otimes id_n)(C_{\mathcal{E}})|\phi\phi\rangle\big\} = \lambda_1 - \max_{|\phi\rangle \in \mathcal{H}_n} \big\{\langle\phi\phi|(T \otimes id_n)(\lambda_1 I - C_{\mathcal{E}})|\phi\phi\rangle\big\}. \tag{11}$$

For convenience, we will now define $X := P_{\mathcal{S}}(T \otimes id_n)(\lambda_1 I - C_{\mathcal{E}})P_{\mathcal{S}}$. Notice that X is positive semidefinite. We now note that

$$\max_{|\phi\rangle \in \mathcal{H}_n} \big\{\langle\phi\phi|(T \otimes id_n)(\lambda_1 I - C_{\mathcal{E}})|\phi\phi\rangle\big\} \leq \max_{|\psi\rangle,|\chi\rangle \in \mathcal{H}_n} \big\{\langle\psi\chi|X|\psi\chi\rangle\big\}$$

trivially by letting $|\psi\rangle = |\chi\rangle = |\phi\rangle$. To see that the opposite inequality holds as well (and hence complete the proof), suppose $|\psi\rangle \neq |\chi\rangle$ and observe that $P_{\mathcal{S}}|\psi\chi\rangle = \frac{1}{2}(|\psi\chi\rangle + |\chi\psi\rangle)$ is a scalar multiple of a symmetric state with Schmidt rank 2. It follows via the Takagi factorization that we can write $P_{\mathcal{S}}|\psi\chi\rangle = \alpha|\rho\rho\rangle + \beta|\sigma\sigma\rangle$ for some $|\rho\rangle, |\sigma\rangle \in \mathcal{H}_n$ and $\alpha, \beta \geq 0$. Suppose without loss of generality that

$$\langle\rho\rho|X|\rho\rho\rangle \geq \langle\sigma\sigma|X|\sigma\sigma\rangle.$$

Then write X in its Spectral Decomposition as $X = \sum_i \lambda_i |v_i\rangle\langle v_i|$ and define the i^{th} component of two vectors ρ' and σ' by $\rho'_i := \sqrt{\lambda_i}|\langle v_i|\rho\rho\rangle|$ and $\sigma'_i := \sqrt{\lambda_i}|\langle\sigma\sigma|v_i\rangle|$. Applying the Cauchy-Schwarz inequality to ρ' and σ' shows

$$|\langle\sigma\sigma|X|\rho\rho\rangle| \leq \sqrt{\langle\rho\rho|X|\rho\rho\rangle}\sqrt{\langle\sigma\sigma|X|\sigma\sigma\rangle} \leq \langle\rho\rho|X|\rho\rho\rangle.$$

Putting all of this together shows that

$$\begin{aligned}
\langle\psi\chi|X|\psi\chi\rangle &= (\alpha\langle\rho\rho| + \beta\langle\sigma\sigma|)X(\alpha|\rho\rho\rangle + \beta|\sigma\sigma\rangle) \\
&= \alpha^2\langle\rho\rho|X|\rho\rho\rangle + \alpha\beta(\langle\rho\rho|X|\sigma\sigma\rangle + \langle\sigma\sigma|X|\rho\rho\rangle) + \beta^2\langle\sigma\sigma|X|\sigma\sigma\rangle \\
&\leq (\alpha^2 + \beta^2)\langle\rho\rho|X|\rho\rho\rangle + \alpha\beta(|\langle\rho\rho|X|\sigma\sigma\rangle| + |\langle\sigma\sigma|X|\rho\rho\rangle|) \\
&\leq (\alpha^2 + 2\alpha\beta + \beta^2)\langle\rho\rho|X|\rho\rho\rangle \\
&= (\alpha + \beta)^2\langle\rho\rho|X|\rho\rho\rangle.
\end{aligned}$$

Thus, if we can prove that $\alpha + \beta \leq 1$ then we are done. To this end, first note that without loss of generality we can assume that $\langle\psi|\chi\rangle$ is real, simply by adjusting the global phase between $|\psi\rangle$ and $|\chi\rangle$ appropriately. Now recall from the Takagi factorization that α and β are the square roots of the eigenvalues of the matrix

$$\begin{aligned}
AA^* &:= \frac{1}{4}\big(|\psi\rangle\overline{\langle\chi|} + |\chi\rangle\overline{\langle\psi|}\big)\big(\overline{|\chi\rangle}\langle\psi| + \overline{|\psi\rangle}\langle\chi|\big) \\
&= \frac{1}{4}\big(|\psi\rangle\langle\psi| + \langle\psi|\chi\rangle(|\chi\rangle\langle\psi| + |\psi\rangle\langle\chi|) + |\chi\rangle\langle\chi|\big).
\end{aligned}$$

It is easily verified that eigenvectors of AA^* are $|\psi\rangle \pm |\chi\rangle$ and the associated eigenvalues are

$$\frac{1}{4}\big(\langle\psi|\chi\rangle^2 \pm 2\langle\psi|\chi\rangle + 1\big).$$

If we add the square roots of these eigenvalues, we get

$$\begin{aligned}
\alpha + \beta &= \frac{1}{2}\sqrt{\langle\psi|\chi\rangle^2 + 2\langle\psi|\chi\rangle + 1} + \frac{1}{2}\sqrt{\langle\psi|\chi\rangle^2 - 2\langle\psi|\chi\rangle + 1} \\
&= \frac{1}{2}\sqrt{(\langle\psi|\chi\rangle + 1)^2} + \frac{1}{2}\sqrt{(\langle\psi|\chi\rangle - 1)^2} \\
&= \frac{1}{2}\big|1 + \langle\psi|\chi\rangle\big| + \frac{1}{2}\big|1 - \langle\psi|\chi\rangle\big| \\
&= 1,
\end{aligned}$$

where the final equality follows from the fact that $-1 \leq \langle\psi|\chi\rangle \leq 1$. The result follows. □

Several bounds and results on the minimum gate fidelity follow immediately from the corresponding results on the $S(1)$-norm derived in [4, 5]. We present a brief selection of these results here for completeness.

Corollary 9. *Let $\mathcal{E} : \mathcal{L}(\mathcal{H}_n) \to \mathcal{L}(\mathcal{H}_n)$ be a quantum channel. Denote the eigenvalues of $P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$ supported on $P_{\mathcal{S}}$ by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{n(n+1)/2}$ (i.e., these are the eigenvalues of $P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$ with $n(n-1)/2$ zero eigenvalues removed). Let α_j be the maximal Schmidt coefficient of the eigenvector corresponding to λ_j. Then*

$$\max_j\{(\lambda_1 - \lambda_j)\alpha_j^2\} \leq \lambda_1 - \mathcal{F}_{\mathcal{E}}^{min} \leq \min\big\{\lambda_1 - \lambda_{n(n+1)/2}, \sum_j (\lambda_1 - \lambda_j)\alpha_j^2\big\}.$$

Proof. The fact that $\lambda_1 - \mathcal{F}_{\mathcal{E}}^{min} \leq \lambda_1 - \lambda_{n(n+1)/2}$ follows immediately from Theorem 8 and the fact that $\|\cdot\|_{S(1)} \leq \|\cdot\|$. The other upper bound of $\lambda_1 - \mathcal{F}_{\mathcal{E}}^{min}$ follows from [4, Theorem 3.3 and Proposition 4.11]. The lower bound can be derived by using the spectral decomposition to write

$$P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}} = \sum_j \lambda_j |v_j\rangle\langle v_j|.$$

If $|v\rangle \in \mathcal{H}_n \otimes \mathcal{H}_n$ is the separable state corresponding to the maximal Schmidt coefficient α_j of $|v_j\rangle$ then

$$\begin{aligned}\langle v|P_{\mathcal{S}}(T \otimes id_n)(\lambda_1 I - C_{\mathcal{E}})P_{\mathcal{S}}|v\rangle &= \sum_i (\lambda_1 - \lambda_i)|\langle v_i|v\rangle|^2 \\ &= (\lambda_1 - \lambda_j)\alpha_j^2 + \sum_{i\neq j}(\lambda_1 - \lambda_i)|\langle v_i|v\rangle|^2 \\ &\geq (\lambda_1 - \lambda_j)\alpha_j^2.\end{aligned}$$

The corresponding lower bound follows by letting j range from 1 to $n(n+1)/2$. □

Remark 10. In the case that $n = 2$, the $S(1)$-norm can be efficiently computed to any desired accuracy via semidefinite programming [5]. As a corollary of this fact, we now have a semidefinite program for efficiently computing $\mathcal{F}_{\mathcal{E}}^{min}$ of qubit channels $\mathcal{E} : \mathcal{L}(\mathcal{H}_2) \to \mathcal{L}(\mathcal{H}_2)$ to any desired accuracy. The primal and dual forms of the semidefinite program in question are as follows:

Primal problem

$$\begin{aligned}\text{minimize:} \quad & \lambda_1 - \mathrm{Tr}\big((\lambda_1 P_{\mathcal{S}} - P_{\mathcal{S}}(T \otimes id_2)(C_{\mathcal{E}})P_{\mathcal{S}})\rho\big) \\ \text{subject to:} \quad & \rho \geq 0, (id_2 \otimes T)(\rho) \geq 0 \\ & \mathrm{Tr}(\rho) = 1\end{aligned}$$

Dual problem

$$\begin{aligned}\text{maximize:} \quad & \lambda_1 - \big\|(T \otimes id_2)(Y) + (P_{\mathcal{S}}(T \otimes id_2)(\lambda_1 I - C_{\mathcal{E}})P_{\mathcal{S}})\big\| \\ \text{subject to:} \quad & Y \geq 0\end{aligned}$$

Using the MATLAB code provided in [5] to solve this semidefinite program, we are able to approximate the distribution of the minimum gate fidelity when $n = 2$. Figure 1 shows

the distribution of $\mathcal{F}_{\mathcal{E}}^{min}$ and $\overline{\mathcal{F}_{\mathcal{E}}}$ when the quantum channel $\mathcal{E}$ is chosen by picking a Haar-uniform unitary $U \in \mathcal{L}(\mathcal{H}_4) \otimes \mathcal{L}(\mathcal{H}_2)$ and then setting $\mathcal{E}(\rho) \equiv \mathrm{Tr}_1(U(|0\rangle\langle 0| \otimes \rho)U^\dagger)$.

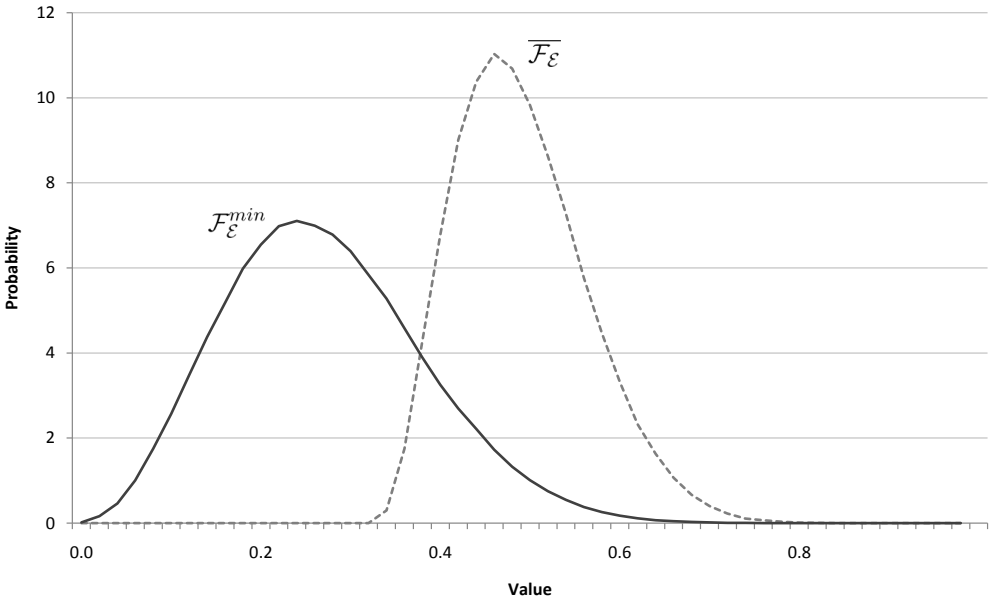

FIGURE 1. Approximate distributions of $\mathcal{F}_{\mathcal{E}}^{min}$ and $\overline{\mathcal{F}_{\mathcal{E}}}$ when $n = 2$, based on $5 \cdot 10^5$ randomly-generated qubit channels.

7. Outlook

We have seen that the quantum gate fidelity of a quantum channel $\mathcal{E}$ is characterized by a particular operator, $P_{\mathcal{S}}(T \otimes id_n)(C_{\mathcal{E}})P_{\mathcal{S}}$. Furthermore, the average and minimum gate fidelities can be expressed in terms of this operator relatively simply, as can the variance of the gate fidelity.

Although the $S(1)$-norm in general is NP-HARD to compute, this does not immediately imply that computing $\mathcal{F}_{\mathcal{E}}^{min}$ is NP-HARD as well, because the operator whose norm is computed in Theorem 8 has a special form (in particular, it is supported on the symmetric subspace). Determining whether or not $\mathcal{F}_{\mathcal{E}}^{min}$ is difficult to compute would be a great step toward a better understanding of gate fidelities. Also, we have provided a semidefinite program that computes $\mathcal{F}_{\mathcal{E}}^{min}$ for any qubit channel $\mathcal{E}$, but it might be possible to do better than this and find an explicit formula for the minimum gate fidelity in this situation.

Acknowledgements. We are grateful to the referees for helpful comments. Thanks are extended to Moritz Ernst for pointing out an error in an early version of Proposition 1. N.J. was supported by an NSERC Canada Graduate Scholarship and the University of Guelph

Brock Scholarship. D.W.K. was supported by Ontario Early Researcher Award 048142, NSERC Discovery Grant 400160 and NSERC Discovery Accelerator Supplement 400233.

References

[1] M. Nielsen and I. Chuang, *Quantum computation and quantum information*. Cambridge University Press (2000).

[2] M. Choi, *Completely positive linear maps on complex matrices*. Linear Algebra Appl. **10**, 285–290 (1975).

[3] E. Magesan, *Depolarizing behavior of quantum channels in higher dimensions*. Quantum Inf. Comput. **11**, 0466–0484 (2011).

[4] N. Johnston and D. W. Kribs, *A family of norms with applications in quantum information theory*. J. Math. Phys. **51**, 082202 (2010).

[5] N. Johnston and D. W. Kribs, *A family of norms with applications in quantum information theory II*. Quantum Inf. Comput. **11** 1 & 2, 104-123 (2011).

[6] A. Uhlmann, *The "transition probability" in the state space of a $*$-algebra*. Rep. Math. Phys. **9**, 273–279 (1976).

[7] R. Jozsa, *Fidelity for mixed quantum states*. J. Modern Opt. **41**, 2315–2323 (1994).

[8] M. Horodecki, P. Horodecki and R. Horodecki, *General teleportation channel, singlet fraction, and quasidistillation*. Phys. Rev. A **60**, 1888 (1999).

[9] M. Nielsen, *A simple formula for the average gate fidelity of a quantum dynamical operation*. Phys. Lett. A **303**, 249–252 (2002).

[10] M. D. Bowdreya, D. K. L. Oia, A. J. Shorta, K. Banaszeka, and J. A. Jones, *Fidelity of single qubit maps*. Phys. Lett. A **294**, 258–260 (2002).

[11] A. Gilchrist, N. K. Langford, and M. A. Nielsen, *Distance measures to compare real and ideal quantum processes*. Phys. Rev. A **71**, 062310 (2005).

[12] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators*. J. Opt. B **7**, S347–S352 (2005).

[13] I. Bengtsson and K. Życzkowski, *Geometry of quantum states: an introduction to quantum entanglement*. Cambridge University Press, Cambridge, UK (2006).

[14] L. H. Pedersen, N. M. Møller, and K. Mølmer, *The distribution of quantum fidelities*. Phys. Lett. A **372**, 7028–7032 (2011).

[15] E. Magesan, R. Blume-Kohout, and J. Emerson, *Gate fidelity fluctuations and quantum process invariants*. Phys. Rev. A **84**, 012309 (2011).

[16] T. Karasawa, J. Gea-Banacloche, and M. Ozawa, *Gate fidelity of arbitrary single-qubit gates constrained by conservation laws*. J. Phys. A: Math. Theor., **42**, 225303 (2009).

[17] H.-T. Lim, Y.-S. Ra, Y.-S. Kim, Y.-H. Kim, and J. Bae, *Gate fidelities, quantum broadcasting, and assessing experimental realization*. E-print: arXiv:1106.5873 [quant-ph]

[18] T. Takagi, *On an algebraic problem related to an analytic theorem of Caratheodory and Fejer*. Japan J. Math. **1**, 83–93 (1924).

[19] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University Press, 1985.

[20] E. Størmer, *Mapping cones of positive maps*. Math. Scand. **108**, 223–232 (2011).

[21] M.-D. Choi, D. W. Kribs, and K. Życzkowski, *Higher-rank numerical ranges and compression problems*. Linear Algebra Appl., **418**, 828–839 (2006).

[22] N. Johnston, D. W. Kribs, V. I. Paulsen and R. Pereira, *Minimal and maximal operator spaces and operator systems in entanglement theory*. J. Funct. Anal. **260** 8, 2407–2423 (2011).

[23] N. Johnston, *Characterizing operations preserving separability measures via linear preserver problems*. Linear Multilinear Algebra **59**, 1171–1187 (2011).

[24] K. Takesaki and J. Tomiyama, *On the geometry of positive maps in matrix algebras*. Math. Zeit. **184**, 101–108 (1983).

[25] F. Benatti, R. Floreanini, and M. Piani, *Non-decomposable quantum dynamical semigroups and bound entangled states*. Open Sys. Inf. Dyn. **11**, 325–338 (2004).

[26] A. Peres, *Separability criterion for density matrices*. Phys. Rev. Lett. **77**, 1413 (1996).

[27] M. Horodecki, P. Horodecki, and R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*. Phys. Lett. A **223**, 1 (1996).
[28] B. M. Terhal, *Detecting quantum entanglement*. J. Theor. Comp. Sci. **287**, 313–335 (2002).
[29] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *A complete family of separability criteria*. Phys. Rev. A **69**, 022308 (2004).
[30] D. Chruściński and A. Kossakowski, *Spectral conditions for positive maps*. Comm. Math. Phys. **290**, 1051-1064 (2009).
[31] R. Horodecki, P. Horodecki, M. Horodecki, and Karol Horodecki, *Quantum entanglement*. Rev. Mod. Phys. **81**, 865–942 (2009).
[32] L. Vandenberghe and S. Boyd, *Semidefinite programming*, SIAM *Review*, 38(1), 49–95 (1996).
[33] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, SpringerVerlag, second corrected edition (1993).
[34] M. Navascués, M. Owari, and M. B. Plenio, *Power of symmetric extensions for entanglement detection*. Phys. Rev. A **80**, 052306 (2009).

Department of Mathematics and Statistics, University of Guelph, Guelph, Ontario N1G 2W1, Canada
E-mail address: njohns01@uoguelph.ca

Department of Mathematics and Statistics, University of Guelph, Guelph, Ontario N1G 2W1, Canada and Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
E-mail address: dkribs@uoguelph.ca