

Process tomography for unitary quantum channels

Gus Gutoski^a, Nathaniel Johnston^b

^a*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada*

^b*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada*

October 11, 2013

Abstract

We study the number of measurements required for quantum process tomography under prior information, such as a promise that the unknown channel is unitary. We introduce the notion of an interactive observable and we show that any unitary channel acting on a d -level quantum system can be uniquely identified among all other channels (unitary or otherwise) with only $O(d^2)$ interactive observables, as opposed to the $O(d^4)$ required for tomography of arbitrary channels. This result generalizes to the problem of identifying channels with at most q Kraus operators, and slight improvements can be obtained if we wish to identify such a channel only among unital channels or among other channels with q Kraus operators. These results are proven via explicit construction of large subspaces of Hermitian matrices with various conditions on rank, eigenvalues, and partial trace. Our constructions are built upon various forms of totally nonsingular matrices.

Keywords: process tomography, unitary channels, high-rank subspaces

1. Introduction

The problem of deducing the action of an unknown quantum channel by gathering statistics from repeated measurement is called *process tomography*. In general, one must measure a set of $O(d^4)$ distinct observables in order to uniquely identify a given channel Φ acting on a d -level quantum system, owing to the fact that the set of all such channels spans an affine space of dimension $d^4 - d^2$.

However, it could be that far fewer observables are required if we are promised that Φ belongs to some prescribed set A of channels or if we only wish to identify Φ among some specific subset B of all possible channels. In other words, we are interested in the following question for various sets $A \subseteq B$ of channels:

Given an unknown channel $\Phi \in A$, what is the minimum number of observables required to ensure that there is no other channel in B with the same measurement statistics as Φ ?

Email addresses: `ggutoski@perimeterinstitute.ca` (Gus Gutoski),
`nathaniel.johnston@uwaterloo.ca` (Nathaniel Johnston)

1.1. Primary results

We show that if Φ is promised to be a *unitary* channel then it suffices to measure only $O(d^2)$ observables in order to uniquely identify Φ among all channels, and that slight improvements can be obtained if we wish to identify Φ only among unital or unitary channels. In particular,

1. $4d^2 - 2d - 4$ observables suffice to identify a unitary among other unitaries. If $d = 2$ then only 6 observables suffice.
2. $5d^2 - 3d - 4$ observables suffice to identify a unitary among all channels.
3. $5d^2 - 4d - 5$ observables suffice to identify a unitary among unital channels.

These results generalize to the problem of identifying channels with at most q Kraus operators; we show that it suffices to measure $O(d^2q + q^2)$ observables, with slight improvements if we wish to identify such a channel only among unital channels or among other channels with q Kraus operators. A detailed statement of these results is given in Theorem 5 of Section 4.4. Several potential extensions of these results are described in Section 7.

1.2. Prior work

Our work is inspired by previous results on the number of observables required for *state* tomography, the study of which was initiated by Heinosaari, Mazzearella, and Wolf [HMW13] who showed that any pure state of a d -level quantum system can be uniquely identified among other pure states with only $O(d)$ observables, as opposed to the $O(d^2)$ required for tomography of an arbitrary state. In particular, $4d - 5$ observables suffice and this bound generalizes to the problem of identifying states with rank at most q among other states with rank at most q .

Chen, Dawkins, Ji, Johnston, Kribs, Shultz, and Zeng investigated the number of observables required in order to identify a given pure state among *all* states [CDJ⁺13]. Those authors showed that $O(d)$ observables suffice even in this more demanding setting. In particular, $4d - 5$ observables no longer suffice but $5d - 7$ observables is sufficient. As in Ref. [HMW13], this bound generalizes to the problem of identifying states with rank at most q among all states. This work was continued by Carmeli, Heinosaari, Schultz, and Toigo [CHST13], who slightly improved the number of observables that suffice in this setting in some cases.

Although there are some results on the number of observables required for process tomography under certain sparsity assumptions [SKM⁺11], we are not aware of any prior work on the number of observables required for process tomography under the promise that the unknown channel is unitary or has few Kraus operators.

Kimmel, da Silva, Ryan, Johnson, and Ohki showed that the unital part of any multi-qubit channel can be deduced from Clifford measurements, which tend to be easier to implement in practice, and that their procedure is robust in the presence of measurement error [KdSR⁺13]. By contrast, our primary goal is to minimize the number of observables required for tomography without regard to how those observables might be implemented. However,

in Section 7.4 we observe that the six observables required for tomography of qubit unitary channels are in fact products of Clifford operators.

1.3. Methods and supplementary results

The primary results of Section 1.1 rest upon several supplementary results on interactive observables, on the construction of subspaces of Hermitian matrices with various conditions on rank, eigenvalues, and partial trace, and on the construction of totally nonsingular matrices with various useful properties.

1.3.1. Interactive observables

Before we can talk of the number of observables required for process tomography it is necessary to clarify the meaning of the word “observable” in this context. In Section 2 we introduce the notion of an *interactive observable* for channels, a special case of which is an ordinary observable for states. The latter specifies a measurement for a state; the former, both an input state for a channel and a measurement for the resulting output.

We claim that every $d^2 \times d^2$ Hermitian matrix can be viewed as an interactive observable for channels acting on a d -level quantum system in the same sense that every $d \times d$ Hermitian matrix can be viewed as an ordinary observable for states of a d -level quantum system.

To this end we observe that an arbitrary $d^2 \times d^2$ Hermitian matrix H can be decomposed into an input-state–measurement pair if and only if H lies in the unit ball of the dual of the diamond norm¹, from which the above claim follows via a simple scaling argument. (See Section 2.1 for details and Section 7.3 for further generalization.) By comparison, it is easily seen that an arbitrary $d \times d$ Hermitian matrix can be decomposed into a binary measurement if and only if it lies in the unit ball of the operator norm.

1.3.2. Subspaces of matrices with rank, eigenvalue, and partial trace conditions

In Section 3 we observe that questions about the number of interactive observables required for process tomography can be reduced to the problem of finding large subspaces of Hermitian matrices with some combination of restrictions on rank, eigenvalues, and partial trace. Detailed statements of our primary result on process tomography and supplementary results on Hermitian subspaces can be found in Section 4. Explicit constructions of these subspaces appear in Section 6.

1.3.3. Totally nonsingular matrices

Our supplementary results on Hermitian subspaces in Section 6 rest upon the existence of various forms of totally nonsingular matrices, proofs of which appear in Section 5.

¹The diamond norm is also known as the *completely bounded 1-norm* or the *completely bounded trace norm*.

1.4. Notation, linear algebra, quantum formalism

We restrict attention throughout the paper to finite-dimensional linear algebra. The symbol \mathbb{M}_d denotes the d^2 -dimensional complex vector space of $d \times d$ matrices with complex entries, which is identified in the usual way with the space of linear operators acting on the d -dimensional complex Euclidean space \mathbb{C}^d .

It is helpful to give separate labels to the different factor spaces in tensor product spaces such as $\mathbb{C}^d \otimes \mathbb{C}^d$ or $\mathbb{M}_d \otimes \mathbb{M}_d$. To this end the Calligraphic letters $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ are used to denote isomorphic copies of \mathbb{C}^d . Tensor products such as $\mathcal{X} \otimes \mathcal{Y}$ are abbreviated to $\mathcal{X}\mathcal{Y}$ so that

$$\mathcal{X}\mathcal{Y} = \mathcal{X} \otimes \mathcal{Y} \simeq \mathbb{C}^d \otimes \mathbb{C}^d \simeq \mathbb{C}^{d^2}.$$

The symbol $L(\mathcal{X})$ denotes the vector space of linear operators acting on \mathcal{X} so that $L(\mathcal{X}) \simeq \mathbb{M}_d$ and

$$L(\mathcal{X}\mathcal{Y}) = L(\mathcal{X} \otimes \mathcal{Y}) \simeq \mathbb{M}_d \otimes \mathbb{M}_d \simeq \mathbb{M}_{d^2}.$$

Linear maps from matrices to matrices of the form $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ are in one-to-one correspondence with elements of $L(\mathcal{Y}\mathcal{X})$ via the *Choi–Jamiołkowski isomorphism*:

$$J(\Phi) = \sum_{i,j=1}^d \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|.$$

Here $\{|1\rangle, \dots, |d\rangle\}$ denotes the standard orthonormal basis of \mathbb{C}^d written in the ket notation.

A linear map $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ is: (a) completely positive if and only if $J(\Phi)$ is positive semidefinite, (b) trace-preserving if and only if $\text{Tr}_{\mathcal{Y}}(J(\Phi)) = I_{\mathcal{X}}$, and (c) unital if and only if $\text{Tr}_{\mathcal{X}}(J(\Phi)) = I_{\mathcal{Y}}$. Moreover, Φ is completely positive if and only if there exist linear operators $A_1, \dots, A_q : \mathcal{X} \rightarrow \mathcal{Y}$ with

$$\Phi : X \mapsto \sum_{i=1}^q A_i X A_i^*.$$

Operators with this property are called *Kraus operators* for Φ . The minimum number of Kraus operators required in any such decomposition of Φ is equal to the rank of the Choi matrix $J(\Phi)$.

Associated with each d -level quantum system is a d -dimensional complex Euclidean space \mathcal{X} . The set of possible *states* of such a system is identified with the set of positive semidefinite matrices $\rho \in L(\mathcal{X})$ with trace equal to one. The set of possible *channels* acting on such a system is identified with the set of completely positive and trace-preserving linear maps $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$. Each *measurement* of such a system with a finite number of outcomes indexed by a is represented by a finite set $\{P_a\} \subset L(\mathcal{X})$ of positive semidefinite matrices with $\sum_a P_a = I$. The probability with which a system in state ρ yields outcome a when measured according to $\{P_a\}$ is given by the inner product $\text{Tr}(P_a \rho)$.

2. Interactive observables

The concept of an observable is familiar in the context of state tomography: every $d \times d$ Hermitian matrix H specifies an *observable* for a d -level quantum system. If that system is in state ρ then the *expectation of measuring H* is the quantity $\text{Tr}(H\rho)$.

Perhaps less widely known is the fact that every $d^2 \times d^2$ Hermitian matrix $H \in L(\mathcal{Y}\mathcal{X})$ can also specify an “observable” for a *channel* acting on a d -level quantum system. Given such a channel $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ the *expectation of measuring H* is the quantity $\text{Tr}(HJ(\Phi))$ —the inner product between H and the Choi matrix $J(\Phi)$ associated with Φ . In the context of process tomography, observables such as H shall be called *interactive observables* in order to distinguish them from observables for states.

2.1. Operational interpretation of interactive observables

What does it mean to measure an interactive observable H for a channel Φ ? To answer this question it is helpful to recall the meaning of measurement of an ordinary observable $H \in L(\mathcal{X})$ on a state $\rho \in L(\mathcal{X})$. If $\|H\| \leq 1$ then it is easy to construct a binary measurement $\{P_\pm\} \subset L(\mathcal{X})$ with $H = P_+ - P_-$. Suppose a system in state ρ is measured according to $\{P_\pm\}$ and suppose that we assign the quantities ± 1 to the measurement outcomes \pm . Then the expected value of this quantity is $\text{Tr}(P_+\rho) - \text{Tr}(P_-\rho) = \text{Tr}(H\rho)$ —the expectation of measuring H . If $\|H\| > 1$ then the expectation of measuring H is simply $\|H\|$ times the expectation of measuring $H/\|H\|$, which, again, is $\text{Tr}(H\rho)$.

For interactive observables on channels, if $H \in L(\mathcal{Y}\mathcal{X})$ is sufficiently small then a more elaborate construction can be used to extract from H a state $\xi \in L(\mathcal{X}\mathcal{Z})$ and a binary measurement $\{P_\pm\} \subset L(\mathcal{Y}\mathcal{Z})$ with the property that

$$\text{Tr}(HJ(\Phi)) = \text{Tr}(P_+(\Phi \otimes \mathbb{1}_{\mathcal{Z}})(\xi)) - \text{Tr}(P_-(\Phi \otimes \mathbb{1}_{\mathcal{Z}})(\xi)).$$

Thus, if we apply Φ to one of two d -level systems in joint state ξ and measure the resulting state $(\Phi \otimes \mathbb{1}_{\mathcal{Z}})(\xi)$ according to $\{P_\pm\}$, assigning the quantities ± 1 to the measurement outcomes \pm as before, then the expected value of this quantity is precisely the inner product $\text{Tr}(HJ(\Phi))$ of H with the Choi matrix $J(\Phi)$ —the expectation of measuring H .

2.2. How to decompose an interactive observable

Given an interactive observable H , how does one compute the associated state ξ and measurement $\{P_\pm\}$? Suppose $H \in L(\mathcal{Y}\mathcal{X})$ is small enough that it can be written $H = Q_+ - Q_-$ for some positive matrices Q_\pm such that $Q_+ + Q_- = I_{\mathcal{Y}} \otimes \rho$ for some state $\rho \in L(\mathcal{X})$. Such a set $\{Q_\pm\}$ has been called a *one-round measuring co-strategy* [GW07], a *1-tester* [CDP09], a *process POVM* [Zim08], and an *interactive measurement* [JUW09]. Each of Refs. [GW07, CDP09, Zim08] offers a proof that any interactive measurement $\{Q_\pm\} \subset L(\mathcal{Y}\mathcal{X})$ can be decomposed into a state $\xi \in L(\mathcal{X}\mathcal{Z})$ and a measurement $\{P_\pm\} \subset L(\mathcal{Y}\mathcal{Z})$ with

$$\text{Tr}(Q_\pm J(\Phi)) = \text{Tr}(P_\pm(\Phi \otimes \mathbb{1}_{\mathcal{Z}})(\xi))$$

for all channels $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$. These proofs are constructive and the construction can be implemented efficiently on a computer.

We are not aware of a succinct formula for $\xi, \{P_{\pm}\}$ in terms of an arbitrary interactive observable H . But such a formula can be derived for the special case in which the state $\rho \in L(\mathcal{X})$ above is the completely mixed state $I_{\mathcal{X}}/d$. In this case we may take

$$\xi = |\phi^+\rangle\langle\phi^+|$$

where $|\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_{\mathcal{X}} |i\rangle_{\mathcal{Z}}$ denotes the canonical maximally entangled pure state. If we let H_{\pm} denote the positive and negative parts of H then the interactive measurement $\{Q_{\pm}\}$ for H can be written

$$Q_{\pm} = H_{\pm} + \frac{I_{\mathcal{Y}\mathcal{X}}/d - H_+ - H_-}{2}$$

and the desired measurement $\{P_{\pm}\}$ is given by normalization and matrix transposition:

$$P_{\pm} = dQ_{\pm}^{\top}.$$

2.3. Our interactive observables may be implemented with a maximally entangled state

Our results on process tomography are not sensitive to scaling. Specifically, the sets of interactive observables presented in the present paper for the purpose of identifying unitary channels can always be assumed to consist entirely of interactive observables H with $\|H\| \leq 1/d$ so that the formulas of Section 2.2 applies for extracting $\xi, \{P_{\pm}\}$ from H . In particular, each of our interactive observables can be implemented by applying Φ to the maximally entangled pure state $|\phi^+\rangle$ —the only difference among our observables is in how the resulting state $(\Phi \otimes \mathbb{1}_{\mathcal{Z}})(|\phi^+\rangle\langle\phi^+|)$ is measured.

In retrospect it is not surprising that a fixed maximally entangled pure input state suffices for process tomography: every channel Φ is uniquely determined by its Choi matrix $J(\Phi)$, which is given by

$$J(\Phi) = d(\Phi \otimes \mathbb{1}_{\mathcal{Z}})(|\phi^+\rangle\langle\phi^+|).$$

2.4. The dual of the diamond norm is the appropriate metric for interactive observables

In Section 2.2 we claimed that a small enough Hermitian matrix $H \in L(\mathcal{Y}\mathcal{X})$ can always be decomposed into a state $\xi \in L(\mathcal{X}\mathcal{Z})$ and measurement $\{P_{\pm}\} \subset L(\mathcal{Y}\mathcal{Z})$. The curious reader might ask, “How small is ‘small enough’?” The answer is that H must lie in the unit ball of the *dual of the diamond norm*.

Specifically, it was shown via semidefinite programming in Ref. [Gut12] that H is in the unit ball of the dual of the diamond norm if and only if it can be written $H = Q_+ - Q_-$ for some interactive measurement $\{Q_{\pm}\}$, from which the claim follows. (An alternate proof of this fact that does not use semidefinite programming follows almost immediately from [JK13, Theorem 2].)

What is the dual of the diamond norm of a Hermitian operator H ? The familiar diamond norm is traditionally defined for linear maps of the form $\Psi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ so let us begin by considering the dual of the diamond norm for linear maps of this form:

$$\|\Psi\|_{\diamond}^* \stackrel{\text{def}}{=} \max_{\|\Phi\|_{\diamond} \leq 1} \langle \Phi, \Psi \rangle.$$

Here the inner product $\langle \Phi, \Psi \rangle$ between two linear maps $\Phi, \Psi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ is defined in the natural way by

$$\langle \Phi, \Psi \rangle \stackrel{\text{def}}{=} \sum_{i,j=1}^{\dim(\mathcal{X})} \text{Tr}(\Phi(|i\rangle\langle j|)^* \Psi(|i\rangle\langle j|)) = \text{Tr}(J(\Phi)^* J(\Psi)).$$

The diamond norm and its dual can also be defined for operators $H \in L(\mathcal{Y}\mathcal{X})$ via the Choi–Jamiołkowski isomorphism. To this end let $\Psi_H : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ be the unique linear map with $J(\Psi_H) = H$. The diamond norm and its dual of H are thus given by

$$\begin{aligned} \|H\|_{\diamond} &\stackrel{\text{def}}{=} \|\Psi_H\|_{\diamond}, \\ \|H\|_{\diamond}^* &\stackrel{\text{def}}{=} \|\Psi_H\|_{\diamond}^*. \end{aligned}$$

3. Reduction to finding large spaces

Now that we have formally defined the concept of an interactive observable we may return to the question of the number of such observables required to uniquely identify a unitary or low-rank channel. Previous works on state tomography began by reducing the problem to one of finding large subspaces of traceless Hermitian matrices of high rank [HMW13] or with a prescribed number of positive eigenvalues [CDJ+13]. Following this lead, we begin by reducing the problem of process tomography to one of finding large subspaces of Hermitian matrices with zero *partial* trace (as opposed to zero trace) and having large rank or a prescribed number of positive eigenvalues.

Let $H_1, \dots, H_m \in L(\mathcal{Y}\mathcal{X})$ be arbitrary $d^2 \times d^2$ Hermitian matrices, which we view as interactive observables for channels acting on a d -level quantum system as discussed in Section 2, and let $\vec{H} = (H_1, \dots, H_m)$ denote an arbitrary ordering of these observables. For any Hermitian matrix $X \in L(\mathcal{Y}\mathcal{X})$ we write

$$\vec{H}(X) = (\text{Tr}(H_1 X), \dots, \text{Tr}(H_m X)) \in \mathbb{R}^m$$

so that for each channel $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ the symbol $\vec{H}(J(\Phi))$ denotes an ordered vector of expectations obtained by measuring each of H_1, \dots, H_m with respect to Φ . Under this notation, a set $\{H_1, \dots, H_m\}$ of interactive observables uniquely identifies channels in A among channels in B if and only if $\vec{H}(J(\Phi)) \neq \vec{H}(J(\Psi))$ for each choice of distinct $\Phi \in A$ and $\Psi \in B$.

Let $\mathbf{V} \subset \mathbf{Q} \subset L(\mathcal{Y}\mathcal{X})$ be Hermitian subspaces of $L(\mathcal{Y}\mathcal{X})$ such that

1. $J(\Phi) - J(\Psi) \in \mathbf{Q}$ for each choice of $\Phi \in A$ and $\Psi \in B$.
2. $J(\Phi) - J(\Psi) \notin \mathbf{V}$ for any choice of distinct channels $\Phi \in A$ and $\Psi \in B$.

A space \mathbf{V} with these properties called a *discriminating subspace* for A, B . Letting \mathbf{V}^{\perp} denote the orthogonal complement of \mathbf{V} within \mathbf{Q} , we claim that any spanning set $\{H_1, \dots, H_m\}$ of \mathbf{V}^{\perp} uniquely identifies channels in A among channels in B .

To see this, let $\vec{H} = (H_1, \dots, H_m)$ be any list of interactive observables such that the space $\mathbf{V} = (\text{span}\{H_1, \dots, H_m\})^\perp$ is a discriminating subspace for A, B . Then for any distinct channels $\Phi \in A, \Psi \in B$ we have

$$\begin{aligned} \vec{H}(J(\Phi)) = \vec{H}(J(\Psi)) &\iff \vec{H}(J(\Phi) - J(\Psi)) = \vec{0} \\ &\iff J(\Phi) - J(\Psi) \in \mathbf{V} \\ &\implies \text{either } \Phi \notin A \text{ or } \Psi \notin B \end{aligned}$$

from which we conclude that $\{H_1, \dots, H_m\}$ uniquely identifies each channel A among channels in B .

Given spaces \mathbf{V}, \mathbf{Q} as above, the number m of interactive observables required to identify channels in A among channels in B is given by

$$m = \dim(\mathbf{V}^\perp) = \dim(\mathbf{Q}) - \dim(\mathbf{V}).$$

This number is minimized when the dimension of \mathbf{Q} is minimal and the dimension of \mathbf{V} is maximal.

It appears that there is little flexibility in the choice of \mathbf{Q} : in this paper we take \mathbf{Q} to be one of the two spaces

$$\mathbf{Q}_{\text{all}} \stackrel{\text{def}}{=} \text{span} \{ J(\Phi) - J(\Psi) \mid \Phi, \Psi : \mathcal{L}(\mathcal{X}) \rightarrow \mathcal{L}(\mathcal{Y}) \text{ are channels} \} \quad (1)$$

$$= \{ Q \in \mathcal{L}(\mathcal{Y}\mathcal{X}) \mid \text{Tr}_{\mathcal{Y}}(Q) = 0_{\mathcal{X}} \}$$

$$\mathbf{Q}_{\text{unital}} \stackrel{\text{def}}{=} \text{span} \{ J(\Phi) - J(\Psi) \mid \Phi, \Psi : \mathcal{L}(\mathcal{X}) \rightarrow \mathcal{L}(\mathcal{Y}) \text{ are unital channels} \} \quad (2)$$

$$= \{ Q \in \mathcal{L}(\mathcal{Y}\mathcal{X}) \mid \text{Tr}_{\mathcal{Y}}(Q) = \text{Tr}_{\mathcal{X}}(Q) = 0 \}$$

having

$$\begin{aligned} \dim(\mathbf{Q}_{\text{all}}) &= d^4 - d^2 \\ \dim(\mathbf{Q}_{\text{unital}}) &= d^4 - 2d^2 + 1 \end{aligned}$$

The difficulty lies in exhibiting large discriminating subspaces $\mathbf{V} \subset \mathbf{Q}$ for A, B ; the remainder of this paper is devoted to this task for various choices of sets A, B .

4. Detailed statement of results

We address the following three questions on process tomography:

How many interactive observables are required in order to uniquely identify...

1. *...channels with at most q Kraus operators among other channels with at most q Kraus operators?*
2. *...channels with at most q Kraus operators among all other channels?*
3. *...unital channels with at most q Kraus operators among all other unital channels?*

In Section 3 we reduced questions of this type to the problem of finding large discriminating subspaces. For each of these three questions we identify a potential class of discriminating subspaces and we assert the explicit constructibility of a subspace in that class. (The constructions themselves are given in Section 6.) Answers to the above questions are given in Section 4.4 after we have enumerated our subspace constructions in Sections 4.1–4.3.

4.1. Question 1: Identification among channels with few Kraus operators

The subspace \mathbf{Q}_{all} of Eq. (1) contains the difference $J(\Phi) - J(\Psi)$ for every choice of channels $\Phi, \Psi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$. If Φ, Ψ each have at most q Kraus operators then their Choi matrices $J(\Phi), J(\Psi)$ each have rank at most q and so it must be that $\text{rank}(J(\Phi) - J(\Psi)) \leq 2q$. Thus, any subspace of $\mathbf{V} \subset \mathbf{Q}_{\text{all}}$ in which every element has rank at least $2q + 1$ is a discriminating subspace for question 1.

Proposition 1 (Subspaces of high-rank matrices with vanishing partial trace). *If $d^2 \geq 2q + 1 \geq 3$ then there exists a subspace $\mathbf{V}_{2q} \subset L(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{2q}) = \begin{cases} (d^2 - 2q)^2 - (d - \lfloor (2q + d - 1)/d \rfloor)^2 & \text{if } d \text{ is odd} \\ (d^2 - 2q)^2 - (d - \lfloor (2q + d - 2)/d \rfloor)^2 & \text{otherwise} \end{cases}$$

such that every nonzero $V \in \mathbf{V}_{2q}$ has rank at least $2q + 1$ and $\text{Tr}_{\mathcal{Y}}(V) = 0_{\mathcal{X}}$.

In the special case of question 1 in which $q = 1$ we are asked to identify unitary channels among other unitary channels. Because every unitary channel is also a unital channel it holds that the difference $J(\Phi) - J(\Psi)$ is contained in the smaller subspace $\mathbf{Q}_{\text{unital}}$ of Eq. (2). In this case, a slight improvement can be obtained if we construct a discriminating subspace within $\mathbf{Q}_{\text{unital}}$.

Proposition 2 (Subspaces of rank-three matrices with two vanishing partial traces). *If $d \geq 3$ then there exists a subspace $\mathbf{V}_{2,\text{unital}} \subset L(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{2,\text{unital}}) = d^4 - 6d^2 + 2d + 5$$

such that every nonzero $V \in \mathbf{V}_{2,\text{unital}}$ has rank at least 3 and $\text{Tr}_{\mathcal{Y}}(V) = \text{Tr}_{\mathcal{X}}(V) = 0$. If $d = 2$ then there exists such a subspace of dimension 3.

Proposition 2 serves to reduce the number of interactive measurements from 9 to 6 in the $d = 2$ case of identifying unitary channels among other unitaries. Otherwise, it reduces that number only by 1.

4.2. Question 2: Identification among all channels

As observed in Section 4.1, the subspace \mathbf{Q}_{all} of Eq. (1) contains the difference $J(\Phi) - J(\Psi)$ for every choice of channels $\Phi, \Psi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$. If Φ has at most q Kraus operators then its Choi matrix $J(\Phi)$ has rank at most q and so it must be that $J(\Phi) - J(\Psi)$ has at most q positive eigenvalues for any choice of channel Ψ . Thus, any subspace of $\mathbf{V} \subset \mathbf{Q}_{\text{all}}$ in which every element has at least $q + 1$ positive eigenvalues is a discriminating subspace for question 2.

Proposition 3 (Subspaces of matrices with many positive eigenvalues and vanishing partial trace). *If $d^2 \geq 2q + 2 \geq 2$ then there exists a subspace $\mathbf{V}_{q+} \subset L(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{q+}) = \begin{cases} d^4 - (4q + 1)d^2 + (4q^2 + 2q) & \text{if } q \geq d \\ d^4 - (4q + 1)d^2 + (4q^2 + 2q) - (d - q)(d - q - 1) & \text{otherwise} \end{cases}$$

such that every nonzero $V \in \mathbf{V}_{q+}$ has at least $q + 1$ positive eigenvalues and $\text{Tr}_{\mathcal{Y}}(V) = 0_{\mathcal{X}}$.

4.3. Question 3: Identification among unital channels

The subspace $\mathbf{Q}_{\text{unital}}$ of Eq. (2) contains the difference $J(\Phi) - J(\Psi)$ for every choice of unital channels $\Phi, \Psi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$. If Φ has at most q Kraus operators then its Choi matrix $J(\Phi)$ has rank at most q and so it must be that $J(\Phi) - J(\Psi)$ has at most q positive eigenvalues for any choice of channel Ψ . Thus, any subspace of $\mathbf{V} \subset \mathbf{Q}_{\text{unital}}$ in which every element has at least $q + 1$ positive eigenvalues is a discriminating subspace for question 3.

Proposition 4 (Subspaces of matrices with many positive eigenvalues and two vanishing partial traces). *If $d^2 \geq 2q + 2 \geq 2$ then there exists a subspace $\mathbf{V}_{q+, \text{unital}} \subset L(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{q+, \text{unital}}) \geq \dim(\mathbf{V}_{q+}) - d^2 + d + 2,$$

where $\dim(\mathbf{V}_{q+})$ is as in Proposition 3, such that every nonzero $V \in \mathbf{V}_{q+, \text{unital}}$ has at least $q + 1$ positive eigenvalues and $\text{Tr}_{\mathcal{Y}}(V) = \text{Tr}_{\mathcal{X}}(V) = 0$.

Indeed, the bound on the dimension of $\mathbf{V}_{q+, \text{unital}}$ in Theorem 4 can be improved slightly when $q \geq d$, but it is too cumbersome to write the precise quantity here: see Section 6.2 for details.

4.4. The number of interactive observables required for process tomography

Our answers to questions 1–3 from the beginning of this section are as follows.

Theorem 5 (Process tomography with $O(d^2)$ interactive observables). *The following hold for channels acting on a d -level quantum system:*

1. $d^4 - d^2 - \dim(\mathbf{V}_{2q})$ interactive observables suffice to identify all channels with at most q Kraus operators among all other channels with at most q Kraus operators.

(Here $\dim(\mathbf{V}_{2q})$ is given in Proposition 1.)

In the special case of identifying unitaries among unitaries ($q = 1$), Proposition 2 further reduces this number to $4d^2 - 2d - 4$ for $d \geq 3$ and from 9 to 6 when $d = 2$.

2. $d^4 - d^2 - \dim(\mathbf{V}_{q+})$ interactive observables suffice to identify all channels with at most q Kraus operators among all other channels.

(Here $\dim(\mathbf{V}_{q+})$ is given in Proposition 3.)

3. $d^4 - 2d^2 + 1 - \dim(\mathbf{V}_{q+, \text{unital}})$ interactive observables suffice to identify all unital channels with at most q Kraus operators among all other unital channels.
 (Here $\dim(\mathbf{V}_{q+, \text{unital}})$ is given in Proposition 4.)

The claims of Section 1.1 are recovered from Theorem 5 in the special case $q = 1$.

5. Notes on total nonsingularity

The remainder of the paper is devoted to the construction of the large subspaces of Hermitian matrices satisfying the various partial trace, rank, and eigenvalue restrictions described in Section 4. Our key building block in the construction of such subspaces (and indeed, one of the building blocks used in each of Refs. [CMW08, HMW13, CDJ+13]) is the notion of *totally nonsingular matrices*—matrices in which every square submatrix is nonsingular.

5.1. Total nonsingularity and high-rank subspaces

One of the most well-known examples of a totally non-singular matrix is a *Vandermonde matrix* [Fal01]

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_d & \alpha_d^2 & \cdots & \alpha_d^{d-1} \end{bmatrix}$$

in which $0 < \alpha_1 < \alpha_2 < \cdots < \alpha_d$. Although only a few other explicit families of totally nonsingular matrices are known, total nonsingularity is a general phenomenon in the sense that the matrices that are not totally nonsingular form a set of measure zero.

The ways in which totally nonsingular matrices are used to construct high-rank subspaces in Refs. [CMW08, HMW13, CDJ+13] are all similar and involve placing the columns of a totally nonsingular matrix along diagonals of matrices. For example, one way to construct a real 9-dimensional subspace $\mathbf{V} \subseteq \mathbb{M}_4$ of Hermitian matrices such that every nonzero $V \in \mathbf{V}$ has $\text{rank}(V) \geq 2$ is to construct matrices with columns of Vandermonde matrices down various diagonals as follows (we use \cdot to denote 0 entries):

$$\begin{aligned} D_1 &= \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} & D_2 &= \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 2 & \cdot & \cdot \\ \cdot & \cdot & 3 & \cdot \\ \cdot & \cdot & \cdot & 4 \end{bmatrix} & D_3 &= \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 4 & \cdot & \cdot \\ \cdot & \cdot & 9 & \cdot \\ \cdot & \cdot & \cdot & 16 \end{bmatrix} \\ D_4 &= \begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} & D_5 &= \begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 2 & \cdot \\ \cdot & \cdot & \cdot & 3 \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} & D_6 &= \begin{bmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}. \end{aligned}$$

Then the 9 Hermitian matrices $\{H_j\}$ defined by $H_j = D_j$ ($1 \leq j \leq 3$), $H_j = D_j + D_j^*$ ($4 \leq j \leq 6$), and $H_j = iD_{j-3} - iD_{j-3}^*$ ($7 \leq j \leq 9$) span a real subspace in which every nonzero matrix has rank at least 2. To see this, notice that in every real linear combination of the H_j 's, there is an upper-right-most diagonal that is nonzero, and that diagonal has at least 2 nonzero entries. The corresponding 2×2 submatrix is thus nonsingular, which implies that the matrix has rank at least 2.

In order to generalize this argument to different dimensions and ranks, we need a way of generating columns (to be placed down various diagonals of the matrices $\{H_j\}$) with the property that their linear combinations do not have “too many” zero entries. The following lemma, which is well-known, shows that totally nonsingular matrices serve this purpose.

Lemma 6. *Let $c \leq r$ be positive integers. If $V \in \mathbb{M}_d$ is such that all of its $r \times c$ submatrices have full rank c , then any linear combination of c columns of V contains at most $r - 1$ zero entries.*

Proof. Suppose for a contradiction that some linear combination of c columns of V contained r or more zero entries. Then the $r \times c$ submatrix of V whose columns correspond to the c columns in the linear combination and whose rows correspond to r of the zero entries must have rank at most $c - 1$, which is a contradiction. \square

5.2. Variations of total nonsingularity combined with linear constraints

While totally nonsingular matrices are useful for the construction of subspaces of high-rank matrices, the subspaces we wish to construct must also satisfy certain partial trace conditions. Thus we don't need totally nonsingular matrices themselves, but rather matrices such that certain subsets of their rows sum to 0, yet their submatrices all have high rank. The following two lemmas serve this purpose—the first lemma when there is one partial trace constraint, the second when there are two.

The first lemma is intuitive enough (albeit slightly technical) that we only provide an “intuitive” and not terribly rigorous proof. The second lemma of this section is much less straightforward, so it is proved rigorously using algebraic geometry techniques. The same techniques could be directly adapted to rigorously prove the first lemma.

Lemma 7. *For all $d, k, m \geq 1$, if we define $f(r) := r - \min(\lfloor r/d \rfloor, k)$ then there exists $V \in \mathbb{M}_{dk+m-1}$ with the following two properties:*

1. *For all $0 \leq j < k$, the sum of rows $jd + 1, jd + 2, \dots, (j + 1)d$ of V equals 0.*
2. *For all $1 \leq r < dk + m$, every $r \times f(r)$ submatrix of V has full rank $f(r)$.*

Proof. Observe that property 2 is satisfied by a generic matrix with property 1. Indeed, suppose first that $m = 1$ and the entries of V are selected uniformly at random from the interval $[0, 1]$ subject to the constraint that every d th row is the negative of the sum of the previous $d - 1$ rows. If $r \geq c$ then, generically, every $r \times c$ submatrix of V will have rank $\min\{r - \ell, c\}$, where ℓ is the number of distinct values of j such that this submatrix contains each of the d rows $jd + 1, jd + 2, \dots, (j + 1)d$ of V . Since $\ell \leq \lfloor r/d \rfloor$, the result in the $m = 1$

case follows by letting $c = r - \lfloor r/d \rfloor$. For the case of general m , simply append $m - 1$ randomly-generated rows to the bottom of V . \square

To help illustrate Lemma 7, we note that in the $d = k = 2, m = 1$ case it says that there exist 4×4 matrices such that the sum of the first two rows equals 0, the sum of the last two rows equals 0, every 1×1 submatrix has rank 1, and every 3×2 submatrix has rank 2 (it also says that every 2×1 submatrix has rank 1 and that every 4×2 submatrix has rank 2, but these properties follow automatically from the 1×1 and 3×2 rank properties). Such a matrix is easily constructed simply by randomly generating the first and third rows, setting the second and fourth rows equal to their negatives, and then verifying that the rank conditions are satisfied. For example, it is easily-verified that the following matrix satisfies all of the requirements:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 2 & 3 & 4 \\ -1 & -2 & -3 & -4 \end{bmatrix}.$$

While Lemma 7 is useful for constructing subspaces of high-rank matrices with vanishing partial trace, we also need to construct subspaces of high-rank matrices with *two* vanishing partial traces. The following lemma serves this purpose.

Lemma 8. *For all $d \geq 1$, if we define $f(r) := \min(r - \lfloor (r-1)/(d-1) \rfloor, (d-1)^2)$ then there exists $V \in \mathbb{M}_{d^2}$ with the following three properties:*

1. *For all $0 \leq j < d$, the sum of rows $jd + 1, jd + 2, \dots, (j+1)d$ of V equals 0.*
2. *For all $0 \leq j < d$, the sum of rows $j + 1, j + 1 + d, j + 1 + 2d, \dots, j + 1 + (d-1)d$ of V equals 0.*
3. *For all $1 \leq r \leq d^2$, every $r \times f(r)$ submatrix of V has full rank $f(r)$.*

Proof. As in the proof of Lemma 7, observe that a generic matrix that satisfies properties 1 and 2 also satisfies property 3. This lemma is perhaps less intuitive than Lemma 7 though, so we prove it a bit more formally.

We begin by noting that the set of matrices satisfying conditions 1 and 2 of the lemma forms an irreducible real algebraic variety $\mathcal{Z} \subseteq \mathbb{R}^{2d^2}$ (the fact that it is irreducible follows from it being a subspace). Let $1 \leq i_1 < i_2 < \dots < i_r \leq d^2$ and $1 \leq j_1 < j_2 < \dots < j_{f(r)} \leq d^2$ be integers, and define $\mathcal{Z}_{i_1 \dots i_r, j_1 \dots j_{f(r)}} \subseteq \mathbb{R}^{2d^2}$ to be the real variety consisting of matrices whose submatrix formed by rows i_1, i_2, \dots, i_r and columns $j_1, j_2, \dots, j_{f(r)}$ has rank strictly less than $f(r)$.

Our goal is to show that

$$\mathcal{Z} \setminus \left(\bigcup_{\substack{1 \leq i_1 < \dots < i_r \leq d^2 \\ 1 \leq j_1 < \dots < j_{f(r)} \leq d^2}} \mathcal{Z}_{i_1 \dots i_r, j_1 \dots j_{f(r)}} \right) \neq \emptyset. \quad (3)$$

Suppose for now, for each fixed $1 \leq i_1 < i_2 < \dots < i_r \leq d^2$ and $1 \leq j_1 < j_2 < \dots < j_{f(r)} \leq d^2$, that $\mathcal{Z} \cap \mathcal{Z}_{i_1 \dots i_r, j_1 \dots j_{f(r)}}$ is a proper subset of \mathcal{Z} . It then follows that it in fact has zero measure in \mathcal{Z} (since \mathcal{Z} is irreducible). Since a finite union of measure zero sets again has measure zero, this implies that

$$\mathcal{Z} \cap \left(\bigcup_{\substack{1 \leq i_1 < \dots < i_r \leq d^2 \\ 1 \leq j_1 < \dots < j_{f(r)} \leq d^2}} \mathcal{Z}_{i_1 \dots i_r, j_1 \dots j_{f(r)}} \right)$$

has zero measure in \mathcal{Z} , which implies Equation (3).

It thus suffices to show that for each fixed $1 \leq i_1 < i_2 < \dots < i_r \leq d^2$ and $1 \leq j_1 < j_2 < \dots < j_{f(r)} \leq d^2$ there exists a matrix \tilde{V} satisfying conditions 1 and 2 of the lemma such that the submatrix of \tilde{V} corresponding to rows i_1, i_2, \dots, i_r and columns $j_1, j_2, \dots, j_{f(r)}$ has full rank $f(r)$. (Henceforth we denote this submatrix by $\tilde{V}_{i_1 \dots i_r, j_1, \dots, j_{f(r)}}$.) The existence of \tilde{V} is straightforward, as the conditions 1 and 2 impose conditions only on $\max\{\lfloor (r-1)/(d-1) \rfloor, r - (d-1)^2\} = r - f(r)$ of the rows of $\tilde{V}_{i_1 \dots i_r, j_1, \dots, j_{f(r)}}$. Thus we are free to set some $f(r) \times f(r)$ submatrix of $\tilde{V}_{i_1 \dots i_r, j_1, \dots, j_{f(r)}}$ to be the identity matrix (which ensures that \tilde{V} has full rank $f(r)$) and then fill in the remaining entries of \tilde{V} arbitrarily, subject to constraints 1 and 2. \square

To help illustrate the above result, we present the following example of a matrix $V \in \mathbb{M}_9$ that satisfies all three conditions of Lemma 8 in the $d = 3$ case:

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ -2 & -4 & -5 & -6 & -7 & -8 & -9 & -10 & -11 \\ 1 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & 100 \\ 1 & 27 & 64 & 125 & 216 & 343 & 512 & 729 & 1000 \\ -2 & -36 & -80 & -150 & -252 & -392 & -576 & -810 & -1100 \\ -2 & -10 & -17 & -26 & -37 & -50 & -65 & -82 & -101 \\ -2 & -30 & -68 & -130 & -222 & -350 & -520 & -738 & -1010 \\ 4 & 40 & 85 & 156 & 259 & 400 & 585 & 820 & 1111 \end{bmatrix}.$$

It is straightforward to verify that: (a) the sum of rows 1, 2, 3 is zero, as is the sum of rows 4, 5, 6 and the sum of rows 7, 8, 9; (b) the sum of rows 1, 4, 7 is zero, as is the sum of rows 2, 5, 8 and the sum of rows 3, 6, 9; and (c) every 1×1 , 2×2 , 4×3 , and 6×4 submatrix of V is nonsingular.

By combining Lemma 7 or 8 with Lemma 6, we are able to construct matrices whose rows sum to zero in ways that play nicely with the partial trace and are also such that linear combinations of their columns contain large numbers of nonzero entries. We make use of such matrices in the next section to construct high-rank subspaces with zero partial trace.

6. Construction of large subspaces of Hermitian matrices

In this section we invoke the preliminary results of Section 5 on totally nonsingular matrices in order to prove Propositions 1–4 of Section 4 on the existence of large subspaces

of Hermitian matrices that satisfy various partial trace, rank, and eigenvalue restrictions. We repeat the statements of those propositions here for readability.

Before proving these results, it will be useful to recall explicitly that elements of $L(\mathcal{Y}\mathcal{X})$ can be thought of as $d \times d$ block matrices, and the maps $\text{Tr}_{\mathcal{X}}(\cdot)$ and $\text{Tr}_{\mathcal{Y}}(\cdot)$ have very simple formulas in terms of the elements of such block matrices:

$$\text{Tr}_{\mathcal{X}} \left(\begin{bmatrix} H_{11} & H_{12} & \cdots & H_{1d} \\ H_{21} & H_{22} & \cdots & H_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ H_{d1} & H_{d2} & \cdots & H_{dd} \end{bmatrix} \right) = \begin{bmatrix} \text{Tr}(H_{11}) & \text{Tr}(H_{12}) & \cdots & \text{Tr}(H_{1d}) \\ \text{Tr}(H_{21}) & \text{Tr}(H_{22}) & \cdots & \text{Tr}(H_{2d}) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Tr}(H_{d1}) & \text{Tr}(H_{d2}) & \cdots & \text{Tr}(H_{dd}) \end{bmatrix} \quad \text{and}$$

$$\text{Tr}_{\mathcal{Y}} \left(\begin{bmatrix} H_{11} & H_{12} & \cdots & H_{1d} \\ H_{21} & H_{22} & \cdots & H_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ H_{d1} & H_{d2} & \cdots & H_{dd} \end{bmatrix} \right) = \sum_{i=1}^d H_{ii}.$$

Since our goal in the proofs of the following propositions is to construct a basis of Hermitian matrices that spans a space of high rank with zero partial trace, it suffices to find such a basis with either $\text{Tr}(H_{ij}) = 0$ for all $1 \leq i, j \leq d$ and all H in the basis, or with $\sum_{i=1}^d H_{ii} = 0_{\mathcal{X}}$ for all H in the basis, or both, depending on which subset of the partial traces we want to vanish.

6.1. Subspaces of high-rank matrices with vanishing partial trace

We now present our results that allow us to construct large subspaces of Hermitian matrices with high rank and zero partial trace. Throughout the proofs of both of these lemmas, we will discuss various diagonals of block matrices, only some of which have any effect on the partial trace. For example, in the $3^2 \times 3^2$ block matrix

$$\left[\begin{array}{ccc|ccc|ccc} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 8 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\ 7 & 8 & 9 & 8 & 7 & 6 & 5 & 4 & 3 \\ \hline 6 & 7 & 8 & 9 & 8 & 7 & 6 & 5 & 4 \\ 5 & 6 & 7 & 8 & 9 & 8 & 7 & 6 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 & 8 & 7 & 6 \\ \hline 3 & 4 & 5 & 6 & 7 & 8 & 9 & 8 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \right],$$

only the diagonals consisting of 7's, 8's, and 9's affect $\text{Tr}_{\mathcal{Y}}$ (in general, only the main diagonal and the $2d - 2$ other nearest diagonals affect $\text{Tr}_{\mathcal{Y}}$), and only the diagonals consisting of 3's, 6's, and 9's affect $\text{Tr}_{\mathcal{X}}$ (in general, only the main diagonal and every d -th diagonal on either side of it affect $\text{Tr}_{\mathcal{X}}$).

Proposition 1 (Subspaces of high-rank matrices with vanishing partial trace). *If $d^2 \geq 2q + 1 \geq 3$ then there exists a subspace $\mathbf{V}_{2q} \subset \mathbf{L}(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{2q}) = \begin{cases} (d^2 - 2q)^2 - (d - \lfloor (2q + d - 1)/d \rfloor)^2 & \text{if } d \text{ is odd} \\ (d^2 - 2q)^2 - (d - \lfloor (2q + d - 2)/d \rfloor)^2 & \text{otherwise} \end{cases}$$

such that every nonzero $V \in \mathbf{V}_{2q}$ has rank at least $2q + 1$ and $\text{Tr}_{\mathcal{Y}}(V) = 0_{\mathcal{X}}$.

Proof. We prove the statement by giving an explicit construction, which is built upon the construction given in [HMW13, Proposition 4] (i.e., the construction that was roughly illustrated in Section 5.1). We begin by taking the basis $\{H_i\}$ of the subspace given without the partial trace condition and then impose the partial trace condition and see how much the dimensionality is reduced. (However, we actually set $\text{Tr}_{\mathcal{X}}(H) = 0_{\mathcal{Y}}$ rather than $\text{Tr}_{\mathcal{Y}}(H) = 0_{\mathcal{X}}$, as this results in a larger subspace—one can then just swap the spaces \mathcal{X}, \mathcal{Y} to get $\text{Tr}_{\mathcal{Y}}(H) = 0_{\mathcal{X}}$.) More specifically, we consider the $(d^2 - 2q)^2$ matrices H_i constructed along diagonals in the proof of [HMW13, Proposition 4] and think of them as $d \times d$ block matrices. In order to ensure that $\text{Tr}_{\mathcal{X}}(H_i) = 0$ for all i , if H_i is defined along a diagonal that consists of the main diagonals of $k \geq 1$ of its subblocks, we place along that diagonal the columns of a matrix described by Lemma 7 (with $m = 1$) rather than the columns of a totally nonsingular matrix.

Since we want any linear combination of the H_i 's to have at least $2q + 1$ nonzero entries, from Lemma 6 and the $m = 1$ case of Lemma 7 we can construct $(dk - 2q) - \lfloor (dk - 2q)/d \rfloor$ such matrices along these “problem” diagonals, rather than the $dk - 2q$ such matrices in the original proof. We thus lose $\lfloor (dk - 2q)/d \rfloor$ matrices along each diagonal that goes through k block diagonals, for a total of

$$\lfloor (d^2 - 2q)/d \rfloor + 2 \sum_{k=1}^{d-1} \lfloor (dk - 2q)/d \rfloor = \begin{cases} (d - \lfloor (2q + d - 1)/d \rfloor)^2 & \text{if } d \text{ is odd} \\ (d - \lfloor (2q + d - 2)/d \rfloor)^2 & \text{if } d \text{ is even} \end{cases}$$

matrices. Since the original subspace without the partial trace condition had dimension $(d^2 - 2q)^2$, the subspace \mathbf{V}_{2q} described after imposing the partial trace condition has the dimensionality specified in the statement of the proposition. \square

Proposition 2 (Subspaces of rank-three matrices with two vanishing partial traces). *If $d \geq 3$ then there exists a subspace $\mathbf{V}_{2,\text{unital}} \subset \mathbf{L}(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{2,\text{unital}}) = d^4 - 6d^2 + 2d + 5$$

such that every nonzero $V \in \mathbf{V}_{2,\text{unital}}$ has rank at least 3 and $\text{Tr}_{\mathcal{Y}}(V) = \text{Tr}_{\mathcal{X}}(V) = 0$. If $d = 2$ then there exists such a subspace of dimension 3.

Proof. We prove the result by giving an explicit construction that arises from modifying the basis given in the proof of Proposition 1. That is, we begin by taking the basis $\{H_i\}$ of

the subspace given with only one partial trace restriction and then impose the other partial trace condition and see how much the dimensionality is reduced.

As before, we think of each H_i as a $d \times d$ block matrix. In order to ensure that $\text{Tr}_{\mathcal{Y}}(H_i) = 0_{\mathcal{X}}$ for all i , if H_i is defined along its main diagonal, we place along that diagonal the columns of a matrix described by Lemma 8 rather than the columns of a matrix described by Lemma 7. Similarly, if H_i is defined along one of the other $2d - 2$ diagonals closest to the main diagonal, we place along that diagonal the columns of a matrix described by Lemma 7 (with $m > 1$ and the rows permuted accordingly so that $\text{Tr}_{\mathcal{Y}}(H_i) = 0_{\mathcal{X}}$) rather than the columns of a totally nonsingular matrix.

Since we want any linear combination of the H_i 's to have at least 3 nonzero entries, from Lemmas 6 and 8 we can construct $(d - 1)^2$ such matrices along the main diagonal (i.e., we lose $d - 2$ matrices), and along the other $2d - 2$ diagonals nearest to the main diagonal we can construct $2(d - 1)(d^2 - d - 2)$ matrices (i.e., we lose $d(d - 1)$ matrices along these diagonal). Since the original subspace \mathbf{V}_2 with just one partial trace constraint had dimension $(d^2 - 2)^2 - (d - 1)^2$, the subspace $\mathbf{V}_{2,\text{unital}}$ described after imposing the second partial trace constraint has dimension $(d^2 - 2)^2 - (d - 1)^2 - (d - 2) - d(d - 1) = d^4 - 6d^2 + 2d + 5$.

The claim about the case $d = 2$ follows from observing the the following 3 block matrices form a basis for a subspace that satisfies all of the given rank and partial trace requirements:

$$\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right], \quad \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ \hline 0 & 2 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{array} \right], \quad \left[\begin{array}{cc|cc} 0 & i & 0 & 0 \\ -i & 0 & 2i & 0 \\ \hline 0 & -2i & 0 & -i \\ 0 & 0 & i & 0 \end{array} \right]. \quad (4)$$

□

6.2. Subspaces of matrices with many positive eigenvalues and vanishing partial trace

We now present our results that allow us to construct large subspaces of Hermitian matrices with many positive eigenvalues. Unlike the proofs in the previous subsection, the matrices considered here are constructed along *anti*-diagonals (i.e., diagonals that run from lower-left to upper-right) rather than standard diagonals. That is, we now follow the approach of [CDJ⁺13, Lemma 2], rather than that of [HMW13, Proposition 4], but our constructions are again more complicated as a result of us requiring that the partial trace of every element of the subspace vanishes.

Note that, in the following propositions, we only consider the upper-triangular part of the anti-diagonals (i.e., the part of the anti-diagonals lying *strictly* above the main diagonal), as the Hermiticity condition determines the lower-triangular entries and all entries along the main diagonal equal 0.

Proposition 3 (Subspaces of matrices with many positive eigenvalues and vanishing partial trace). *If $d^2 \geq 2q + 2 \geq 2$ then there exists a subspace $\mathbf{V}_{q+} \subset \text{L}(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{q+}) = \begin{cases} d^4 - (4q + 1)d^2 + (4q^2 + 2q) & \text{if } q \geq d \\ d^4 - (4q + 1)d^2 + (4q^2 + 2q) - (d - q)(d - q - 1) & \text{otherwise} \end{cases}$$

such that every nonzero $V \in \mathbf{V}_{q+}$ has at least $q + 1$ positive eigenvalues and $\text{Tr}_{\mathcal{Y}}(V) = 0_{\mathcal{X}}$.

Proof. We prove the statement by giving an explicit construction of such a subspace, which is built upon the construction given in [CDJ⁺13, Lemma 2]. In fact, our construction is exactly the same, but with just one change in order to impose the partial trace condition.

As usual, we think of each matrix $V \in \mathbf{V}_{q+}$ as a $d \times d$ block matrix. We construct a basis $\{H_i\}$ of \mathbf{V}_{q+} as in [CDJ⁺13] by placing columns of a totally nonsingular matrix along the upper-triangular part of anti-diagonals. In order to ensure that $\text{Tr}_{\mathcal{Y}}(H_i) = 0_{\mathcal{X}}$ for all i , however, we subtract $\text{Tr}_{\mathcal{Y}}(H_i)$ from the top-left block of H_i . Two examples of such matrices H_i in the $d = 3$ case are as follows:

$$\left[\begin{array}{ccc|ccc|ccc} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad \left[\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

In the left matrix, we initially placed $[1, 2, 3, 4]$ along one of the upper-triangular anti-diagonals, then we adjusted the other entries to enforce Hermiticity and the partial trace constraint. In the right matrix, we similarly placed $[1, 2]$ along one of the upper-triangular anti-diagonals, but in this case, when we enforced the Hermiticity and partial trace constraints, the $(2, 3)$ - and $(3, 2)$ -entries of the matrix were forced to equal 0.

The rightmost example above illustrates the one and only case where forcing $\text{Tr}_{\mathcal{Y}}(H_i) = 0_{\mathcal{X}}$ has any effect on the proof that these matrices are linearly independent and every matrix in this subspace has at least $q + 1$ positive and $q + 1$ negative eigenvalues: when the anti-diagonal that defines H_i goes through the top-left $d \times d$ sub-block. In this case, all entries within that block of H_i are forced to be 0, which reduces the number of distinct matrices H_i that we can construct along that anti-diagonal (for example, the matrix on the right above is *not* included in the basis of our subspace when $q = 1$, since the zeros at the $(2, 3)$ - and $(3, 2)$ -entries cause it to only have 1 positive and 1 negative eigenvalue). There are $d(d - 1)/2$ upper-triangular anti-diagonals that intersect the top-left block. However, $\min(2q, d(d - 1)/2)$ of those anti-diagonals are of length $\leq q$ and do not have an associated matrix H_i . For each of the other anti-diagonals that intersect the top-left block, we lose $2\min(z, \ell - q)$ matrices, where z is the number of entries along that upper-triangular anti-diagonal within the top-left block and ℓ is the length of that anti-diagonal. Thus we remove a total of $(d - q - 1)\max\{d - q, 0\}$ matrices from the set $\{H_i\}$ in order to not violate the eigenvalue requirement. Since the dimension of the subspace constructed in this way in [CDJ⁺13] *without* the partial trace restriction was $d^4 - (4q + 1)d^2 + (4q^2 + 2q)$, the result follows. \square

Throughout the proof of the following proposition, we will repeatedly refer to the quantity

$$L_{d,k} \stackrel{\text{def}}{=} \begin{cases} \lfloor \frac{k+1}{2} \rfloor & \text{if } k < d \\ \lfloor \frac{2d-k-1}{2} \rfloor & \text{if } k \geq d \end{cases}.$$

That is, $L_{d,k}$ is the length of the k th upper-triangular anti-diagonal of a $d \times d$ matrix, just as in [CDJ⁺13]. Note that we count the upper-triangular anti-diagonals from left to right, so that the $(1,2)$ -entry is the first upper-triangular anti-diagonal, the $(1,3)$ -entry is the second upper-triangular anti-diagonal, the $(1,4)$ - and $(2,3)$ -entries together make up the third upper-triangular anti-diagonal, and so on. For a $d \times d$ matrix, there are $2d - 3$ distinct upper-triangular anti-diagonals.

Proposition 4 (Subspaces of matrices with many positive eigenvalues and two vanishing partial traces). *If $d^2 \geq 2q + 2 \geq 2$ then there exists a subspace $\mathbf{V}_{q+,\text{unital}} \subset L(\mathcal{Y}\mathcal{X})$ of $d^2 \times d^2$ Hermitian matrices of dimension*

$$\dim(\mathbf{V}_{q+,\text{unital}}) \geq \dim(\mathbf{V}_{q+}) - d^2 + d + 2,$$

where $\dim(\mathbf{V}_{q+})$ is as in Proposition 3, such that every nonzero $V \in \mathbf{V}_{q+,\text{unital}}$ has at least $q + 1$ positive eigenvalues and $\text{Tr}_{\mathcal{Y}}(V) = \text{Tr}_{\mathcal{X}}(V) = 0$.

Before proving this proposition, we note that the bound on $\dim(\mathbf{V}_{q+,\text{unital}})$ that we actually prove is slightly better than stated above when $q \geq d$. Indeed, if we define

$$\mathcal{I}_q \stackrel{\text{def}}{=} \{k \in \{1, 2, \dots, 2d - 3\} : L_{d^2,dk} \geq q + 1\} \quad (5)$$

then we show that there exists such a subspace $\mathbf{V}_{q+,\text{unital}}$ with $\dim(\mathbf{V}_{q+,\text{unital}}) = \dim(\mathbf{V}_{q+}) - 2 \sum_{k \in \mathcal{I}_q} L_{d,k}$ when $q \geq d$, and it is straightforward to show that $2 \sum_{k \in \mathcal{I}_q} L_{d,k} \leq d^2 - d - 2$ in this case.

Proof. Once again, we prove this result by explicitly constructing a basis of such a subspace. Our construction uses the basis $\{H_i\}$ constructed in the proof of Proposition 3 as a starting point. As before, we think of these matrices as $d \times d$ block matrices. To enforce the requirement that $\text{Tr}_{\mathcal{X}}(H_i) = 0_{\mathcal{Y}}$ for all i , we add to the top-left entry of each block of H_i the negative of the trace of that block. Applying this procedure to the same two matrices considered in the $d = 3$ case in the proof of Proposition 3 results in the following two matrices:

$$\left[\begin{array}{ccc|ccc|ccc} 0 & 0 & -1 & 0 & 0 & 0 & -3 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline -3 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad \left[\begin{array}{ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right].$$

In the left matrix, the only change is that the $(1, 7)$ - and $(7, 1)$ -entries of the matrix now equal -3 . The right matrix, however, now consists entirely of zeroes. As before, there is only one case where this procedure affects the proof, and that is when the anti-diagonal that defines H_i goes through the top-left corner of a block (as in the example on the right above). In this case, that entry of H_i is forced to be 0, which reduces the number of distinct matrices H_i that we can construct along that anti-diagonal by 2 (one real matrix and one imaginary matrix).

There are $d(d-1)/2$ top-left corners of blocks in the upper-triangular portion of H , however we only remove a matrix from our basis if the anti-diagonal going through that top-left corner has length $\geq q+1$. In other words, we remove $2 \sum_{k \in \mathcal{I}_q} L_{d,k}$ matrices, where \mathcal{I}_q is as in (5). However, if $q < d$ then the anti-diagonals hitting the top-left corner of one of these blocks (the $(1, 2)$ -block) have already been removed by the requirement that $\text{Tr}_{\mathcal{Y}}(H_i) = 0_{\mathcal{X}}$ from Proposition 3, so we add back in 2 matrices. Furthermore, it is straightforward to verify that $2 \sum_{k \in \mathcal{I}_q} L_{d,k} = d^2 - d$ when $q < d$ and $2 \sum_{k \in \mathcal{I}_q} L_{d,k} \leq d^2 - d - 2$ when $q \geq d$, so the result follows. \square

7. Directions for future research

7.1. Generalization to arbitrary affine spaces of states

The questions considered in this work can be viewed as questions about state tomography on certain subsets of states. Using process tomography to uniquely identify unitary channels among unitary channels is in some sense equivalent to using state tomography to uniquely identify maximally entangled bipartite pure states among maximally entangled bipartite pure states. In other words, we can think of it as performing state tomography on the intersection of the set of pure states and the affine space of operators with completely mixed partial trace.

This line of thinking raises a natural question: can we answer uniqueness questions for tomography when we restrict attention to affine spaces other than the space of operators with completely mixed partial trace? We do not have a detailed answer for this question, but we can make some observations.

First, some work in this area has already been done: it was shown in Ref. [HMW13, Proposition 9] that for any manifold \mathcal{P} with real dimension $d(\mathcal{P})$ almost all families of $2d(\mathcal{P}) + 1$ observables uniquely determine elements of \mathcal{P} among elements of \mathcal{P} .

For example, the space of unitary channels acting on \mathbb{M}_d is a real manifold of dimension $d^2 - 1$, so almost any family of $2d^2 - 1$ interactive observables uniquely identifies unitary channels among unitary channels. Remarkably, this quantity is smaller than the $4d^2 - 2d - 4$ interactive observables that were shown to suffice in item 1 of Theorem 5! However, our proof of Theorem 5 is constructive; no explicit set of $2d^2 - 1$ interactive observables is known to uniquely identify unitary channels among other unitary channels.

Second, the above technique does not tell us anything about how many measurements can be used to uniquely determine elements of \mathcal{P} (such as the set of unitary channels) among a *different* set (such as the set of *all* quantum channels). To get general results in this

direction, we simply use the fact that if $\mathbf{Q}, \mathbf{V} \subseteq \mathbb{M}_{d^2}$ are two subspaces, then $\dim(\mathbf{Q} \cap \mathbf{V}) = \dim(\mathbf{Q}) + \dim(\mathbf{V}) - \dim(\mathbf{Q} + \mathbf{V})$.

To illustrate this approach, let \mathbf{V} be the subspace of operators with at least 2 positive eigenvalues of dimension $d^4 - 5d^2 + 6$ constructed in Ref. [CDJ⁺13] and let $\mathbf{Q} = \mathbf{Q}_{\text{all}}$ be the subspace (1) of operators with vanishing partial trace of dimension $d^4 - d^2$. Using the fact that $\dim(\mathbf{Q}_{\text{all}} + \mathbf{V}) \leq d^4$, we see that

$$\begin{aligned} \dim(\mathbf{Q}_{\text{all}} \cap \mathbf{V}) &\geq (d^4 - 5d^2 + 6) + (d^4 - d^2) - d^4 \\ &= d^4 - 6d^2 + 6 \end{aligned}$$

It then follows from the reduction of Section 3 that there is a set of $(d^4 - d^2) - (d^4 - 6d^2 + 6) = 5d^2 - 6$ interactive observables that uniquely identify unitary channels among all channels, which is slightly worse than the $5d^2 - 3d - 4$ interactive observables that were shown in the present paper to suffice for this task.

7.2. Process tomography of no-signaling channels

A channel $\Phi : L(\mathcal{X}_1 \mathcal{X}_2) \rightarrow L(\mathcal{Y}_1 \mathcal{Y}_2)$ acting on two d -level quantum systems is *no-signaling* if the output of the channel on each system is independent of the input to the channel on the other system. This condition is nicely characterized by the linear constraints

$$\text{Tr}_{\mathcal{Y}_b}(J(\Phi)) = Q_b \otimes I_{\mathcal{X}_b} \text{ for some } Q_b, \text{ for each } b \in \{1, 2\}$$

on the Choi matrix $J(\Phi)$. Thus, the reduction of Section 3 can be used to bound the number of interactive observables needed to identify channels among no-signaling channels by finding discriminating subspaces \mathbf{V} of $\mathbf{Q}_{\text{no-sig}}$ where

$$\mathbf{Q}_{\text{no-sig}} \stackrel{\text{def}}{=} \text{span} \{ J(\Phi) - J(\Psi) \mid \Phi, \Psi \text{ are no-signaling channels} \}.$$

However, the task of constructing large subspaces of high-rank matrices within $\mathbf{Q}_{\text{no-sig}}$ is considerably more complicated than that of constructing similar spaces within \mathbf{Q}_{all} or $\mathbf{Q}_{\text{unital}}$. Whereas $\mathbf{Q}_{\text{all}}, \mathbf{Q}_{\text{unital}}$ have only one or two vanishing partial trace constraints, $\mathbf{Q}_{\text{no-sig}}$ has several additional partial trace constraints.

Our experience is that each additional constraint adds considerably to the complication of constructing high-rank subspaces based on totally nonsingular matrices. While this method could in principle yield a significant improvement in the number of interactive observables needed to identify no-signaling channels, the question seems to call out for a different approach.

7.3. Tomography of multi-round quantum strategies

A *quantum strategy* is a specification of the actions of one party in a multi-party interaction involving the exchange of multiple rounds of quantum messages among the parties. Channels arise as a special case of strategies in which only one round of messages is exchanged. The strategy formalism was introduced in Refs. [GW07, CDP08, CDP09] wherein it was shown that a matrix $Q \in L(\mathcal{Y}_1 \cdots \mathcal{Y}_r \mathcal{X}_1 \cdots \mathcal{X}_r)$ represents an r -round strategy for

input spaces $\mathcal{X}_1, \dots, \mathcal{X}_r$ and output spaces $\mathcal{Y}_1, \dots, \mathcal{Y}_r$ if and only if Q is positive semidefinite and

$$\mathrm{Tr}_{\mathcal{Y}_r \dots \mathcal{Y}_i}(Q) = Q_i \otimes I_{\mathcal{X}_r \dots \mathcal{X}_i} \text{ for some } Q_i, \text{ for each } i = 1, \dots, r.$$

Quantum strategies are therefore intimately related to no-signaling channels in that the above constraints also characterize the Choi matrices of channels of the form

$$\Phi : L(\mathcal{X}_1 \cdots \mathcal{X}_r) \rightarrow L(\mathcal{Y}_1 \cdots \mathcal{Y}_r)$$

that act on r distinct d -level quantum systems and are no-signaling from system j to system i for each $1 \leq i < j \leq r$.

An important difference between strategies and no-signaling channels (or any other type of channel) is that channel tomography is achieved by preparing an input state and measuring the output. By contrast, tomography for r -round quantum strategies introduces the need to prepare r input systems and process r output systems in sequence, with future inputs possibly depending on previous outputs. In other words, the “observables” required for strategy tomography are themselves full-blown, multi-round strategies.

At first glance this complication might seem intractable. In order to perform tomography on a multi-round strategy one must deduce not only how the strategy acts on various input states, but also how it acts when various *channels* are applied to its outputs and then subsequently returned to it as inputs in future rounds.

However, strategies that measure other strategies have appeared previously in the literature under the names *r-round measuring co-strategy* [GW07] and *r-tester* [CDP09]. The discussion of Section 2 generalizes readily in light of this prior work. Specifically, one can show that:

1. An arbitrary $d^{2r} \times d^{2r}$ Hermitian matrix H can be viewed as an “ r -round interactive observable” for a strategy that exchanges a d -level quantum system r times in sequence.
2. If H is small enough then one can extract from H a collection of objects—an initial state, a sequence of channels with memory, and a measurement for the final system—that describe the behaviour of the observable operationally.
3. Such an extraction is possible if and only if H lies in the unit ball of the *dual of the strategy r -norm* presented in Ref. [Gut12].

Thus, as with no-signaling channels in Section 7.2, one can employ the reduction of Section 3 and search for large discriminating subspaces of \mathbf{Q}_r where

$$\mathbf{Q}_r \stackrel{\text{def}}{=} \text{span} \{Q - Q' \mid Q, Q' \text{ are } r\text{-round strategies}\}.$$

In short: the task of formalizing the notion of an r -round interactive observable is not the bottleneck that thwarts attempts to bound the number of observables needed for strategy tomography. Rather, the bottleneck lies in the same place as with no-signaling channels and other types of channel—in the ability (or lack thereof) to construct large subspaces of high-rank matrices that also satisfy a myriad of partial trace constraints.

7.4. Experimentally-friendly interactive observables

One of the drawbacks of our approach to process tomography is that the interactive observables obtained from Theorem 5 do not necessarily have a nice form—they might not be Clifford operators, they could be non-local, and so on. Hence, they might be difficult to implement in the laboratory. It would be interesting to consider the number of interactive observables required to reconstruct unitary channels under certain additional “niceness” restrictions such as these.

In order to illustrate the type of result that would be desirable we consider the $d = 2, q = 1$ case of Theorem 5.1, which says that six interactive observables suffice to uniquely determine unitary qubit channels among unitary qubit channels. We now show that we can in fact find six interactive observables for this purpose that are both local and Clifford.

To this end our goal is to find six linearly independent Hermitian local Clifford operators $O_1, \dots, O_6 \in \mathbb{M}_2 \otimes \mathbb{M}_2$ with two vanishing partial traces that are each orthogonal to the three operators (4) presented in the proof of Proposition 2. The following are six such operators:

$$\begin{aligned} O_1 &= X \otimes Z & O_2 &= H \otimes Y & O_3 &= (1 - i)S^\dagger HS \otimes SX \\ O_4 &= Y \otimes Z & O_5 &= ZHZ \otimes X & O_6 &= (1 - i)SHS^\dagger \otimes XS, \end{aligned}$$

where X, Y, Z are the Pauli operators and H, S are the Clifford operators with standard basis representations

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

This construction of O_1, \dots, O_6 is *ad hoc*, and it is not clear whether it can be generalized to the other cases of Theorem 5.

As described in Section 2.2, each of these interactive observables specifies a measurement on a maximally entangled input state, which is not nice. It is not difficult to see that these interactive observables could be measured using only experimentally-friendly product state inputs. However, this product state implementation essentially consists of measuring all twelve degrees of freedom and then throwing away half of the resulting information in order to compile the results into the six observables required for tomography. Obviously, nothing is gained by such an exercise.

Acknowledgements

The authors thank Marcus da Silva, John Watrous, and Bei Zeng for helpful conversations. Research at the Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. GG also acknowledges support from CryptoWorks21. NJ is supported by the Natural Sciences and Engineering Research Council of Canada.

References

- [CDJ⁺13] Jianxin Chen, Hillary Dawkins, Zhengfeng Ji, Nathaniel Johnston, David W. Kribs, Frederic Shultz, and Bei Zeng. Uniqueness of quantum states compatible with given measurement results. *Physical Review A*, 88:012109, 2013. arXiv:1212.3503 [quant-ph].
- [CDP08] Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti. Quantum circuits architecture. *Physical Review Letters*, 101:060401, 2008. arXiv:0712.1325 [quant-ph].
- [CDP09] Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009. arXiv:0904.4483 [quant-ph].
- [CHST13] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Tasks and premises in quantum state determination. arXiv:1308.5502 [quant-ph], 2013.
- [CMW08] Toby S. Cubitt, Ashley Montanaro, and Andreas Winter. On the dimension of subspaces with bounded Schmidt rank. *Journal of Mathematical Physics*, 49:022107, 2008. arXiv:0706.0705 [quant-ph].
- [Fal01] Shaun M. Fallat. Bidiagonal factorizations of totally nonnegative matrices. *American Mathematical Monthly*, 108:697–712, 2001.
- [Gut12] Gus Gutoski. On a measure of distance for quantum strategies. *Journal of Mathematical Physics*, 53(3):032202, 2012. arXiv:1008.4636 [quant-ph].
- [GW07] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th ACM Symposium on Theory of Computing (STOC 2007)*, pages 565–574, 2007. arXiv:quant-ph/0611234.
- [HMW13] Teiko Heinosaari, Luca Mazzarella, and Michael M. Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318:355–374, 2013. arXiv:1109.5478 [quant-ph].
- [JK13] Nathaniel Johnston and David W. Kribs. Duality of entanglement norms. *Houston Journal of Mathematics*, to appear, 2013. arXiv:1304.2328 [quant-ph].
- [JUW09] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pages 534–543, 2009. arXiv:0905.1300 [quant-ph].
- [KdSR⁺13] Shelby Kimmel, Marcus da Silva, Colm Ryan, Blake Johnson, and Thomas Ohki. Robust extraction of tomographic information via randomized benchmarking. arXiv:1306.2348 [quant-ph], 2013.
- [SKM⁺11] A. Shabani, R. L. Kosut, M. Mohseni, H. Rabitz, M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White. Efficient measurement of quantum dynamics via compressive sensing. *Physical Review Letters*, 106:100401, 2011. arXiv:0910.5498 [quant-ph].
- [Zim08] Mário Ziman. Process positive-operator-valued measure: A mathematical framework for the description of process tomography experiments. *Physical Review A*, 77(6):062112, 2008. arXiv:0802.3862 [quant-ph].