

Hypothesis testing on invariant subspaces of the symmetric group: part I. Quantum Sanov's theorem and arbitrarily varying sources

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2014 J. Phys. A: Math. Theor. 47 235303

(<http://iopscience.iop.org/1751-8121/47/23/235303>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 129.187.254.46

This content was downloaded on 26/01/2015 at 09:04

Please note that [terms and conditions apply](#).

Hypothesis testing on invariant subspaces of the symmetric group: part I. Quantum Sanov's theorem and arbitrarily varying sources

J Nötzel

Lehrstuhl für Theoretische Informationstechnik, Technische Universität München,
D-80290 München, Germany

E-mail: janis.noetzel@tum.de

Received 11 November 2013, revised 16 March 2014

Accepted for publication 18 March 2014

Published 20 May 2014

Abstract

We report a proof of the quantum Sanov theorem by the elementary application of basic facts about representations of the symmetric group, together with a complete characterization of the optimal error exponent in a situation where the null hypothesis is given by an arbitrarily varying quantum source instead. Our approach differs from previous ones in two ways. First, it supports a reasoning inspired by the 'method of types'. Second, the measurement scheme we propose to distinguish the two alternatives not only does that job asymptotically perfectly, but also yields additional information about the null hypothesis. An example of that is given. The measurement is composed of projections onto permutation-invariant subspaces, thus providing a direct link between one of the most basic tasks in quantum information on the one hand and fundamental objects in representation theory on the other. We additionally connect to the representation theory by proving a relation between Kostka numbers and quantum states, and to state estimation via a generalization of a well-known spectral estimation theorem to non-i.i.d. sequences.

Keywords: hypothesis testing, representation theory, arbitrarily varying source, Sanov theorem, Stein's lemma, Kostka numbers

PACS numbers: 03.67.-a, 02.50.Tt

1. Introduction

The importance of the symmetric group in quantum Shannon information is inherently connected to the central idea of using an information carrying or transmitting system several times in order to defeat noise. This approach naturally introduces an action of the symmetric group into any model within that theory. On these pages, we will therefore put a clear focus on representations of S_n while almost completely ignoring its commutant, which is, in our case, e.g. a representation of the unitary group.

We will connect two fundamental concepts: hypothesis testing and invariant subspaces of the symmetric group. This also leads to new insights concerning the notion of a quantum method of types.

We will now briefly introduce the two concepts, starting with hypothesis testing. More specifically, we will consider asymmetric hypothesis testing, in the setting of Stein's lemma.

Stein's lemma is one of the fundamental statements in information theory. It gives precise bounds on the probability of correctly identifying the state of a system at hand in situations where it is guaranteed that the actual state is chosen from a set of two states (I and II). The underlying assumption is that infinitely many copies of the system in the exact same state can be prepared, and then measured jointly. The measurement should then identify the true state of the system. The situation is not symmetric: while it is desired to identify state I only with a constant non-negative probability, the probability of correctly identifying state II goes to one asymptotically fast, and the optimal exponent is quantified in Stein's lemma.

In the case that the system at hand is described by quantum theory, the first proof of the direct part of the corresponding quantum Stein's lemma was given by Hiai and Petz in [27]. Soon after, Ogawa and Nagaoka [33] completed the proof by showing the converse. The topic of quantum hypothesis testing has also led to many other developments, and there have been different variants of the proof of Stein's lemma and extensions to more general scenarios. We shall point out some of the landmarks in a roughly chronological order: Hayashi [23] extended the earlier results and related the quantum relative entropy between two states to the classical relative entropy between the distributions of the (not necessarily binary) measurement results for specific measurements acted upon the states. He also presented a specific class of measurements, which he defined using the commutant of the standard representation of S_n on $(\mathbb{C}^d)^{\otimes n}$, the representation of the special linear group obtained from representing each d by d invertible matrix A as $A^{\otimes n}$.

Our definition of measurement differs from his approach foremost in the very clear and explicit choice of parameters that we use to describe our measurements, and the explicit connection to basic concepts in the representation theory of S_n . We hope that this will increase the applicability of methods from representation theory to quantum Shannon information theory.

Hayashi also investigated the quantum Stein's lemma directly in [24], namely with an information-spectrum approach. This work, which also uses basic ingredients from [23], also further clarifies the connection between the statistics of measurements performed on asymptotically many copies of quantum states and the relative entropy of the respective states. His results are of high generality, and could in principle be used to directly prove an i.i.d. version of a quantum version of Sanov's theorem as well, despite the fact that he did not attribute that specific name to his result.

Meanwhile, Nagaoka gave a much simpler proof of the converse part of Stein's lemma in [34]. Later, Ogawa and Hayashi together investigated the interplay between the different rates of convergence of the two errors. The generalization to the ergodic case was done by Bjelaković and Siegmund-Schultze in [7], and was later generalized to the case of a stationary

(instead of i.i.d.) hypothesis by Bjelaković *et al* in [9]. The quantum Sanov theorem was, independent of Hayashi’s work [24], proven by Bjelaković *et al* in [8] and extended to the stationary case in [9].

Another approach is that of Audenaert *et al* [3], who were concerned with asymmetric hypotheses testing. Their results contain the quantum Sanov theorem as a corollary. These results were extended to correlated states by Hiai, Mosonyi and Ogawa in [26].

It was noticed in several of these papers that the choice of the optimal POVM depends on the reference state (state I), and this turns out to be no different in our approach.

A complete estimation scheme that is based on the representation theory of the symmetric group, including its large deviation behaviour, has also been described in [30].

Lately, an important generalizations of Stein’s lemma has been given for the case where the alternative hypothesis consists of a sequence of sets of states satisfying certain stability property results by Brandao and Plenio [11], and their results were extended to the case of restricted measurements in [10].

Let us now state the most basic task that is to be performed in hypothesis testing: given two states $\rho, \sigma \in \mathcal{S}(\mathbb{C}^d)$ and $\nu \in (0, 1)$, determine

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \left(\min_{0 \leq P \leq \mathbb{1}^{\otimes n}} \{ \text{tr}\{P\sigma^{\otimes n}\} : \text{tr}\{P\rho^{\otimes n}\} \geq 1 - \nu \} \right). \quad (1)$$

The quantity $\min_{0 \leq P \leq \mathbb{1}^{\otimes n}} \{ \text{tr}\{P\sigma^{\otimes n}\} : \text{tr}\{P\rho^{\otimes n}\} \geq 1 - \nu \}$ is usually abbreviated as $\beta_{\nu,n}(\rho, \sigma)$ and named the ‘type two error’. The statement of the quantum Stein’s lemma is then:

$$\forall \nu \in (0, 1) : \quad \lim_{n \rightarrow \infty} \frac{1}{n} \log(\beta_{\nu,n}(\rho, \sigma)) = -D(\rho \parallel \sigma). \quad (2)$$

In case we want to distinguish more subtle hypotheses, we have to adjust this definition. In our case, it will be sufficient to look at the following: For a state $\sigma \in \mathcal{S}(\mathbb{C}^d)$, $\nu \in (0, 1)$ and a sequence $\Delta := (\mathfrak{S}_n)_{n \in \mathbb{N}}$ of sets such that $\mathfrak{S}_n \subset \mathcal{S}((\mathbb{C}^d)^{\otimes n})$, we wish to investigate the quantity

$$\beta_{\nu,n}(\Delta, \sigma) := \min_{0 \leq P \leq \mathbb{1}^{\otimes n}} \{ \text{tr}\{P\sigma^{\otimes n}\} : \inf_{\omega \in \mathfrak{S}_n} \text{tr}\{P\omega\} \geq 1 - \nu \}. \quad (3)$$

Our main result (which we state in a much more explicit way later due to intended applications to other problems) can then be formulated as follows.

Theorem 1. *First, if $\Delta = (\{\rho^{\otimes n}\}_{\rho \in \mathfrak{S}})_{n \in \mathbb{N}}$ for some set $\mathfrak{S} \subset \mathcal{S}(\mathbb{C}^d)$, then*

$$\forall \nu \in (0, 1), \quad \lim_{n \rightarrow \infty} \frac{1}{n} \log(\beta_{\nu,n}(\Delta, \sigma)) = - \inf_{\rho \in \mathfrak{S}} D(\rho \parallel \sigma). \quad (4)$$

Second, if $\Delta = (\{\rho_{s^n}\}_{s^n \in \mathfrak{S}^n})_{n \in \mathbb{N}}$, where $\rho_{s^n} := \otimes_{i=1}^n \rho_{s_i}$ and each $\rho_{s_i} \in \mathfrak{S}$ for some set $\mathfrak{S} \subset \mathcal{S}(\mathbb{C}^d)$, then

$$\forall \nu \in (0, 1), \quad \lim_{n \rightarrow \infty} \frac{1}{n} \log(\beta_{\nu,n}(\Delta, \sigma)) = - \inf_{\rho \in \text{conv}(\mathfrak{S})} D(\rho \parallel \sigma). \quad (5)$$

Remark 1. The optimal tests are, in both settings, essentially given by projections onto suitably chosen invariant subspaces of the symmetric group.

The first result in theorem 1 is usually referred to as the ‘quantum Sanov theorem’. We will call the second scenario hypothesis testing for an arbitrarily varying quantum source (sometimes abbreviated as AVQS in the following), where the terminology ‘arbitrarily varying source’ is taken from the classical literature and refers to the sequence Δ in that setting. This model has been investigated first in [20] for the case of two sets of classical probability distributions over a set. Their proof is based on the ‘method of types’.

The ‘method of types’ is best described by Csiszár in [18]. The method is based on a study of the relevant quantities in a given communication scenario on *frequency typical sets*, meaning sets of words of length n that are each composed of only a finite number of symbols, and each symbol occurs a constant number of times in each word. It is clear that such sets are invariant under a joint permutation of the symbols in each word. The success of the method can be read from the fact that it ultimately ended up having its own name. Approaching a given Shannon-information theoretic problem by looking at types can be considered opposed to looking at sets on which one controls the empirical averages of the functions that are of interest in a given problem.

The only stringent attempt to generalize the method of types to the quantum setting that is known to the author is presented in [22] and [4], where the group theoretic structure is presented in great detail. Certainly, also [12] is inspired by that idea.

The methods that were further successfully applied often only use spectral estimation, which already reveals important connections between representation theory and quantum states [13–15]. They are well suited to derive, e.g., estimates of the spectra of states through a basic estimate described in the literature¹ or entropic inequalities. On a more general level, recent results [16, 17, 35] show that there is an enormously fruitful connection between representation theory and the structure of multiparty states. Unfortunately, the quantum method of types as such was not applied or developed any further and could thus not even be used to give proofs for such basic tasks as hypothesis testing, which are both simple and at the very heart of quantum Shannon information theory. At this point, we clearly distinguish between applying the structure given by representation theory as was successfully done in [23] and a reasoning in terms of anything comparable to classical types. We thus now make an explicit choice of ‘types’ that singles out certain invariant subspaces of the symmetric group, and then show that with this choice we can prove our theorem 1. We hope that this will give new thrust to the idea of ‘quantum types’.

At present, it seems not totally clear what such a theory should look like. The relevant parameters will have to be found by subsequently proving the important theorems in quantum Shannon information theory. For the time being, we shall restrict ourselves to considering decompositions $\mathbb{1}^{\otimes n} = \sum_i P_i$ on $(\mathbb{C}^d)^{\otimes n}$ where each P_i is an orthogonal projection onto an irreducible subspace of the natural action of S_n on $(\mathbb{C}^d)^{\otimes n}$, and further $\text{tr}\{P_i P_j\} = 0$ for $i \neq j$. We then consider the set $\{P_i\}_i$ as a POVM, which is to replace the frequency typical subsets from the classical theory. An outline of our approach will now be given.

Despite the above-mentioned drawbacks, the methods from classical information theory were taken over to the quantum case with great success, e.g. in the form of ‘frequency typical subspaces’ that arise from choosing a particular orthonormal basis that is labelled by a classical alphabet, and then by looking at the linear span of all elementary tensor products of n of these basis vectors that are built up from the same number of each of the basis vectors. Closely related is the study of isotypical subspaces in the n -fold tensor product of \mathbb{C}^d . Like typical sets in the classical case, both of the above classes of subspaces are permutation invariant.

This work combines the two approaches by exploiting the fact that every frequency typical subspace can be decomposed into subspaces that are irreducible under the action of the permutation group.

¹ The result we refer to has a long history that is explained in more detail in [12]. According to [12], it first appeared in [2], was then independently proven in [29], later appeared in [25] with a shortened proof, and was, at last, restated in [13], again with the (obtained independently from [25]) shortened version of the proof. We would like to add to this history that it also follows directly from the much earlier work [37].

As mentioned already, the action of the commutant of S_n on the frequency typical subspaces will be insignificant in every single one of the proofs given here. Its exact role will therefore also be addressed in future work.

The basic idea behind the paper is to look, for a given orthonormal basis $\{e_i\}_{i=1}^d$ and a ‘frequency’ or ‘type’ (a non-negative function $f : \{1, \dots, d\} \rightarrow \mathbb{N}$ satisfying $\sum_i f(i) = n$), at representations of the symmetric group S_n on the frequency typical subspaces

$$V_f := \text{span}(\{e_{i_1} \otimes \dots \otimes e_{i_n} : |\{k : i_k = i\}| = f(i) \text{ for all } i\}).$$

Since these are invariant under permutations, they naturally split up into different isotypical subrepresentations $V_{f,\lambda}$ (where λ denote Young tableaux and some $V_{f,\lambda}$ may not contribute to the above decomposition, meaning that $V_{f,\lambda} = \{0\}$ for some pairs (f, λ))

$$V_f = \bigoplus_{\lambda} V_{f,\lambda}. \tag{6}$$

Given a state σ with eigenvalues $t_1 \geq t_2 \geq \dots \geq t_d > 0$, we may now pick one of its eigenbases for the definition of the V_f . It is then straightforward to show that for the orthogonal projections $P_{f,\lambda}$ onto the $V_{f,\lambda}$, the estimate

$$\text{tr}\{P_{f,\lambda}\sigma^{\otimes n}\} \approx \dim(F_{\lambda}) \cdot 2^{-n \sum_i \frac{1}{n} f(i) \log t_i} \tag{7}$$

$$\approx 2^{n(H(\frac{1}{n}\lambda) - \sum_i \frac{1}{n} f(i) \log t_i)} \tag{8}$$

is valid, where $\dim(F_{\lambda})$ is the dimension of the irreducible representation of S_n corresponding to λ and $H(\frac{1}{n}\lambda) = -\sum_i \frac{1}{n} \lambda_i \log(\frac{1}{n} \lambda_i)$ is the entropy of the normalized Young tableau. It turns out that, for $\lambda \approx n \cdot \text{spec}(\rho)$ and $f(i) \approx n \cdot \langle e_i, \rho e_i \rangle \forall i \in [d]$ for some arbitrary second state ρ , we get

$$\text{tr}\{P_{f,\lambda}\sigma^{\otimes n}\} \approx 2^{-nD(\rho\|\sigma)}. \tag{9}$$

It then remains for us to investigate the behaviour of the functions $(f, \lambda) \mapsto \text{tr}\{P_{f,\lambda}\rho^{\otimes n}\}$ and determine where they attain their maximum for a fixed ρ . Luckily it turns out that the maximum lies indeed around the values we have already chosen above, and this is sufficient for a proof of the direct part of the hypothesis testing problem in both cases.

For the sake of completeness, we prove the converse parts in both of our problems by resorting to a reasoning that is based on the method we just outlined above. A crucial ingredient in this part of our proof is the permutation invariance of the sets of states that we are trying to discriminate. This enables one to assume that an arbitrary test is permutation invariant as well, and ultimately this provides the link between an arbitrary test and the performance of tests that are made up from projections onto the $P_{f,\lambda}$.

Outline

The paper is structured as follows. We first fix some basic notation in section 2 and state a few preliminaries in section 3.

We then state our results in section 4, in a very technical fashion compared to theorem 1. Theorems 2 and 4 provide a proof for theorem 1, while theorem 3 makes the connection to the Kostka numbers and lemma 2 provides a more general formula for (spectral) state estimation via projections onto isotypical projections in the sense of the results mentioned in our footnote 1. Our additional theorem 5 is a straightforward generalization of the robustification lemma in [1]. In this version, it can be abbreviated as: any POVM element on $\mathcal{B}((\mathbb{C}^d)^{\otimes n})$ that detects all elementary products states $\rho^{\otimes n}$ with a high probability is close to the identity, whence has poor performance when used as the POVM element in a binary test

for distinguishing between the two hypotheses ‘entangled state’ versus ‘separable state’. The proof of the theorem also reveals that our method could benefit from further refinement.

The rest of the paper is devoted to the proofs of these statements, the proof of lemma 2 being implicit in that of theorem 4.

The proof of theorem 5 suggests that there is still some important information to be gained by using POVMs that are made up from irreducible projections, whereas before we used only invariant ones.

2. Notation

All Hilbert spaces are assumed to have finite dimensions and are over the field \mathbb{C} . The set of linear operators from \mathcal{H} to \mathcal{H} is denoted $\mathcal{B}(\mathcal{H})$. The adjoint of $b \in \mathcal{B}(\mathcal{H})$ is marked by a star and is written b^* .

$\mathcal{S}(\mathcal{H})$ is the set of states, i.e. positive semi-definite operators with trace (the trace function on $\mathbb{B}(\mathcal{H})$ is written tr) 1 acting on the Hilbert space \mathcal{H} . Pure states are given by projections onto one-dimensional subspaces. A vector $x \in \mathcal{H}$ of length one spanning such a subspace will therefore be referred to as a state vector, and the corresponding state will be written $|x\rangle\langle x|$. For a finite set \mathbf{X} , the notation $\mathfrak{P}(\mathbf{X})$ is reserved for the set of probability distributions on \mathbf{X} , and $|\mathbf{X}|$ denotes its cardinality. For any $n \in \mathbb{N}$, we define $\mathbf{X}^n := \{(x_1, \dots, x_n) : x_i \in \mathbf{X} \forall i \in \{1, \dots, n\}\}$; we also write x^n for the elements of \mathbf{X}^n . Given such an element, $N(\cdot|x^n)$ denotes its type, and it is defined through $N(x|x^n) := |\{i : x_i = x\}|$.

For any natural number L , we define $[L]$ to be the shortcut for the set $\{1, \dots, L\}$.

The von Neumann entropy of a state $\rho \in \mathcal{S}(\mathcal{H})$ is given by

$$S(\rho) := -\text{tr}(\rho \log \rho), \tag{10}$$

where $\log(\cdot)$ denotes the base two logarithm which is used throughout the paper.

Given two states $\rho, \sigma \in \mathcal{S}(\mathbb{C}^d)$, the relative entropy of them is defined as

$$D(\rho\|\sigma) := \begin{cases} \text{tr}\{\rho(\log(\rho) - \log(\sigma))\}, & \text{if } \text{supp}(\rho) \subset \text{supp}(\sigma). \\ \infty, & \text{else} \end{cases} \tag{11}$$

Another way of measuring the distance between quantum states is obviously given by using the one-norm, which obeys:

$$\|\rho - \sigma\| := 2 \max_{0 \leq P \leq \mathbb{1}} \text{tr}\{P(\rho - \sigma)\}. \tag{12}$$

We now fix our notation for the representation of theoretic objects and state some basic facts.

The symbols λ, μ will be used to denote Young frames. The set of Young frames with at most $d \in \mathbb{N}$ rows and $n \in \mathbb{N}$ boxes is denoted $\mathbb{Y}_{d,n}$.

For any given n , the representation of S_n we will consider is the standard representation on $(\mathbb{C}^d)^{\otimes n}$ that acts by permuting tensor factors. Throughout, the dimension d of our basic quantum system will remain fixed.

The unique complex vector space carrying the irreducible representation of S_n corresponding to a Young tableau λ will be written F_λ .

The multiplicity of an irreducible subspace of our representation corresponding to a Young frame λ is denoted $m_{\lambda,n}$, and this quantity can be upper bounded by $m_{\lambda,n} \leq (2n)^{d^2}$ (see [12]).

For $\lambda \in \mathbb{Y}_{d,n}$, $\bar{\lambda} \in \mathfrak{P}([d])$ is defined by $\bar{\lambda}(i) := \lambda_i/n$. If $\rho \in \mathcal{S}(\mathbb{C}^d)$ has the spectrum $s \in \mathfrak{P}([d])$ (in the case that ρ has degenerate eigenvalues we count them multiple times!), then it will always be assumed that $s(1) \geq \dots \geq s(d)$ holds and the distance between a spectrum s and a Young frame $\lambda \in \mathbb{Y}_{d,n}$ is measured by $\|\bar{\lambda} - s\| := \sum_{i=1}^d |\bar{\lambda}(i) - s(i)|$. The distance between two probability distributions $p, q \in \mathfrak{P}([d])$ will be measured by $\|p - q\| := \sum_i |p(i) - q(i)|$.

The Kostka numbers $K_{f,\lambda}$ are as defined in, e.g., Fulton’s book [21], pages 25–26.

We now define two important entropic quantities. Given a finite set \mathbf{X} and two probability distributions $r, s \in \mathfrak{P}(\mathbf{X})$, we define the relative entropy $D(r||s)$ by

$$D(r||s) := \begin{cases} \sum_{x \in \mathbf{X}} r(x) \log(r(x)/s(x)), & \text{if } s \gg r \\ \infty, & \text{else} \end{cases} \quad (13)$$

In the case that $D(r||s) = \infty$, for a positive number $a > 0$, we use the convention $2^{-aD(r||s)} = 0$. The relative entropy is connected to $\|\cdot\|$ by Pinsker’s inequality $D(r||s) \geq \alpha \|r - s\|^2$, where $\alpha := 1/2 \ln(2)$.

The entropy of $r \in \mathfrak{P}(\mathbf{X})$ is defined by the formula

$$H(r) := - \sum_{x \in \mathbf{X}} r(x) \log(r(x)). \quad (14)$$

Throughout, we will have one fixed state $\sigma \in \mathcal{S}(\mathbb{C}^d)$ with a (non-unique) decomposition $\sigma = \sum_{i=1}^d t_i |\tilde{e}_i\rangle\langle \tilde{e}_i|$, and the pinching of an arbitrary state $\rho \in \mathcal{S}(\mathbb{C}^d)$ to the orthonormal basis $\{|\tilde{e}_i\rangle\}_{i=1}^d$ will be given by $\sum_{i=1}^d |\tilde{e}_i\rangle\langle \tilde{e}_i| \rho |\tilde{e}_i\rangle\langle \tilde{e}_i|$ and induces the probability distribution $\tilde{r}_\rho \in \mathfrak{P}([d])$ through $\tilde{r}_\rho(i) := \langle \tilde{e}_i, \rho \tilde{e}_i \rangle$. It is important for the understanding of this paper to keep in mind that the equality $D(\rho||\sigma) = -H(\text{spec}(\rho)) - \sum_{i=1}^d \tilde{r}_\rho(i) \log(t_i)$ holds.

We shall also need some notions on convex sets, which we borrow from [38], and that are suited for dealing with convex sets on finite dimensional normed spaces $(V, \|\cdot\|)$ over the field of real or complex numbers. Let $F \subset V$ be convex. $x \in F$ is said to be a relative interior point of F if there is $r > 0$ such that $B(x, r) \cap \text{aff}F \subset F$. Here, $B(x, r)$ denotes an open ball of radius r with a center x , and $\text{aff}F$ stands for the affine hull of F . The set of relative interior points of F is called the relative interior of F and is denoted by $\text{ri}F$. The relative boundary of F , $\text{rebd}F$, is the set difference between the closure of F and $\text{ri}F$.

For a set $A \subset V$ and $\delta \geq 0$, we define the parallel set or the blow-up $(A)_\delta$ of A by

$$(A)_\delta := \{x \in V : \|x - y\| \leq \delta \text{ for some } y \in A\}. \quad (15)$$

For a subset $B \subset \mathbb{R}^n$ or $B \subset \mathbb{C}^n$ we denote its convex hull by $\text{conv}(B)$.

3. Definitions and preliminary results

Let $n \in \mathbb{N}$ be fixed for the moment. The most important technical definition for this work is that of frequency-typical subspaces V_f of $(\mathbb{C}^d)^{\otimes n}$. These arise from choosing a fixed orthonormal basis $\{e_i\}_{i=1}^d$ of \mathbb{C}^d , choosing a frequency f (a function $f : [d] \rightarrow \mathbb{N}$ satisfying $\sum_{i=1}^d f(i) = n$), setting $T_f := \{(i_1, \dots, i_n) : |\{i_k : i_k = j\}| = f(j) \forall j \in [d]\}$, and defining

$$V_f := \text{span}(\{e_{i_1} \otimes \dots \otimes e_{i_n} : (i_1, \dots, i_n) \in T_f\}). \quad (16)$$

They have been widely used in quantum information theory, but they share one very nice property that does not seem to have been exploited yet: they are invariant under permutations. From this property it immediately follows that

$$V_f = \bigoplus_{\lambda} V_{f,\lambda}, \quad (17)$$

where each $V_{f,\lambda}$ is just a direct sum of irreducible representations corresponding to λ that is contained entirely within V_f .

A fundamental representation theoretic quantity is intimately connected to them: the Kostka numbers. In fact, it holds that $K_{f,\lambda} = 0 \Leftrightarrow V_{f,\lambda} = \{0\}$, both by definition

of the Kostka numbers and by application of Young symmetrizers as described in [36], pages 254-258.

Also, we are going to employ the following estimate taken from [19] (lemma 2.3), which is valid for all frequencies $f : [d] \rightarrow \mathbb{N}$ that satisfy $\sum_{i=1}^d f(i) = n$:

$$\frac{1}{(n+1)^d} 2^{nH(\bar{f})} \leq |T_f| \leq 2^{nH(\bar{f})}. \tag{18}$$

We will also need lemma 2.7 from [19]:

Lemma 1. *If, for \mathbf{A} , a finite alphabet, and $p, q \in \mathfrak{P}(\mathbf{A})$ we have $|p - q| \leq \Theta \leq 1/2$, then*

$$|H(p) - H(q)| \leq -\Theta \log \frac{\Theta}{|\mathbf{A}|}. \tag{19}$$

Another very important estimate is the following one (a derivation can be found in, e.g., [32]):

$$2^{n(H(\bar{\lambda}) - \frac{2d^6}{n} \log(2n))} \leq \dim F_\lambda \leq 2^{nH(\bar{\lambda})} \quad (\lambda \in \mathbb{Y}_{d,n}). \tag{20}$$

4. Main results

All results are stated with the underlying Hilbert space being \mathbb{C}^d . Our main result is the finding of a sequence of projections that succeeds in detecting each one of a set $\mathfrak{S} = \{\rho_s\}_{s \in \mathbf{S}}$ of quantum states with the probability going to one, while having the lowest possible probability of detecting another state $\sigma \notin \mathfrak{S}$. We only give the proof in the case of a nonsingular σ , since the singular case can, in dependence of the set $\{\rho_s\}_{s \in \mathbf{S}}$, either be treated identically by the reduction of the dimension of the underlying system or because an optimal test is already given by projecting onto the usual frequency typical subspaces corresponding to σ . This reasoning applies to the case of the AVQS as well.

Our technical formulation of the quantum Sanov theorem for i.i.d. hypotheses reads as follows.

Theorem 2. *Let $\mathfrak{S} = \{\rho_s\}_{s \in \mathbf{S}} \subset \mathcal{S}(\mathbb{C}^d)$ and $\sigma = \sum_{i=1}^d t_i |\tilde{e}_i\rangle\langle \tilde{e}_i| \in \mathcal{S}(\mathbb{C}^d)$, where all $t_i > 0$ are given. We will use the abbreviations $r_s := r_{\rho_s}$ for the spectra of the states of our set and $\tilde{r}_s := \tilde{r}_{\rho_s}$ for the distributions that are induced by pinching them to the eigenbasis of σ . Let a sequence $(P_n)_{n \in \mathbb{N}}$ of projections defined by*

$$P_n := \sum_{(\bar{f}, \bar{\lambda}) \in \Lambda_\varepsilon} P_{\bar{f}, \bar{\lambda}}^n, \tag{21}$$

where the frequency typical subspaces are defined with respect to $\{\tilde{e}_i\}_{i=1}^d$ and

$$\Lambda_\varepsilon := \{(p, q) \in \mathfrak{P}([d] \times [d]) \mid \exists s \in \mathbf{S} : \|p - \tilde{r}_s\| \leq \varepsilon \text{ and } \|q - r_s\| \leq \varepsilon\} \tag{22}$$

and the \tilde{r}_s are the probability distributions defined by $\tilde{r}_s(i) := \langle \tilde{e}_i, \rho_s \tilde{e}_i \rangle$. For this sequence, both

$$\inf_{s \in \mathbf{S}} \text{tr}\{P_n \rho_s^{\otimes n}\} \geq 1 - 2^{-n(\alpha \varepsilon^2 - \frac{d^2}{n} \log(2n))} \tag{23}$$

and

$$\frac{1}{n} \log \text{tr}\{P_n \sigma^{\otimes n}\} \leq -\inf_{s \in \mathbf{S}} D(\rho_s \| \sigma) + \Theta(n, \varepsilon, d, \sigma) \tag{24}$$

are true. In addition, for every $0 \leq A \leq \mathbb{1}^{\otimes n}$ satisfying $\inf_{s \in \mathbb{S}} \text{tr}\{A_n \rho_s^{\otimes n}\} \geq 1 - \nu$ (for some $\nu \in (0, 1)$), it holds that

$$-\inf_{s \in \mathbb{S}} D(\rho_s \| \sigma) - \Theta'(n, \nu, d) \leq \frac{1}{n} \log \text{tr}\{A_n \sigma^{\otimes n}\}. \tag{25}$$

The functions Θ and Θ' are defined by

$$\Theta(n, \varepsilon, d, \sigma) := \frac{d^2}{n} \log(2n) + \varepsilon |\log(\varepsilon/d)| + d\varepsilon \cdot \max_i |\log t_i|, \tag{26}$$

$$\Theta'(n, \nu, d) := \Theta(n, n^{-\frac{1}{4}}, d) - \frac{2d^6}{n} \log(2n) + \frac{1}{n} \log \left(\frac{1 - \nu - 2^{-\alpha\sqrt{n}}}{(2n)^{2d^2}} \right). \tag{27}$$

This proves the quantum Stein's lemma by replacing ε with a suitably chosen sequence $(\varepsilon_n)_{n \in \mathbb{N}}$ that satisfies $\varepsilon_n = \frac{1}{\sqrt{\alpha}} \sqrt{\frac{1}{n} \log(\nu) + \frac{d^2}{n} \log(2n)}$ for all $n \in \mathbb{N}$.

Remark 2. By the linearity of the trace, this implies that we can distinguish the hypotheses $\text{conv}(\{\rho_s^{\otimes n}\}_{s \in \mathbb{S}})$ and $\sigma^{\otimes n}$ at the same rate.

Using theorem 2, we can prove the following result that relates the Kostka numbers to quantum states:

Theorem 3. First, if $K_{f,\lambda} > 0$, then there exists a quantum state with spectrum $\bar{\lambda}$ and pinching \bar{f} .
 Second, if ρ is a quantum state with spectrum r_ρ and pinching \tilde{r}_ρ , then for every $\varepsilon > 0$ there exists $N \in \mathbb{N}$, and for all $n \geq N$ there is $\lambda \in \mathbb{Y}_{d,n}$ and a corresponding frequency such that $\|\bar{\lambda} - r_\rho\| \leq n^{-1/4}$ and $\|\bar{f} - \tilde{r}_\rho\| \leq n^{-1/4}$ and $K_{f,\lambda} > 0$.

Our next result concerns the arbitrarily varying quantum source. The proof of this theorem rests on the proof of theorem 2, so that the functions and objects defined in that theorem are used here as well.

Theorem 4. Under the same preliminaries as above we have: for a finite set $\mathfrak{S}' = \{\rho_s\}_{s \in \mathbb{S}}$ and with the projections P_n defined as in theorem 2 using the set $\mathfrak{S} := \text{conv}(\mathfrak{S}')$, the estimates

$$\text{tr}\{P_n \rho_{s^n}\} \geq 1 - 2^{-n\alpha\varepsilon^2 + \frac{2d^2+|\mathbb{S}|}{n} \log(2n)} \tag{28}$$

and

$$\frac{1}{n} \log \text{tr}\{P_n \sigma^{\otimes n}\} \leq - \min_{\rho \in \text{conv}(\mathfrak{S}')} D(\rho \| \sigma) + \Theta(n, \varepsilon, d, \sigma) + \frac{|\mathbb{S}|}{n} \log(2n) \tag{29}$$

and for every operator $0 \leq A_n \leq \mathbb{1}^{\otimes n}$ satisfying $\min_{s^n \in \mathbb{S}^n} \text{tr}\{A_n \rho_{s^n}\} \geq 1 - \nu$ for some $\nu \in (0, 1)$ we have

$$-\min_{\rho \in \text{conv}(\mathfrak{S}')} D(\rho \| \sigma) - \Gamma(n, \nu, d, \sigma) \leq \frac{1}{n} \log \text{tr}\{A_n \sigma^{\otimes n}\} \tag{30}$$

where

$$\Gamma(n, \nu, d, \sigma) := \Theta(n, n^{-1/4}, d, \sigma) + \Gamma'(n, \nu, d) + \frac{8d^6}{n} \log(2n) \tag{31}$$

$$\Gamma'(n, \nu, d) := \frac{1}{n} \log \left[\left(1 - \nu - 2^{-n[\alpha(n^{-1/4} - 2|\mathbb{S}|n^{-1}) - \frac{|\mathbb{S}| - 2d^2}{n} \log(2n)]} \right) (2n)^{-8d^2} \right]. \tag{32}$$

This proves theorem 1 by replacing ε with $\varepsilon_n := \frac{1}{\sqrt{\alpha}} \sqrt{\frac{1}{n} \log(\nu) + \frac{d^2+|\mathbb{S}|}{n} \log(2n)}$.

In the case that $|\mathcal{S}| = \infty$, the following is true: for the sequence $(\delta_n)_{n \in \mathbb{N}}$ defined by $\delta_n := 12n^{-1/4d^2}$ ($n \in \mathbb{N}$) and the depolarizing channel $\mathcal{N}_{\delta_n} : \mathcal{B}(\mathbb{C}^d) \rightarrow \mathcal{B}(\mathbb{C}^d)$, $a \mapsto (1 - \delta_n)a + \delta_n \frac{1}{d} \mathbb{1}$ we have

$$\inf_{s^n \in \mathcal{S}^n} \text{tr}\{\mathcal{N}_{\delta_n}^{\otimes n}(P_n)\rho_{s^n}\} \geq 1 - 2^{-n(\alpha \varepsilon^2 - \frac{d^2 + \sqrt{n}}{n} \log(2n))} \tag{33}$$

and

$$\text{tr}\{\mathcal{N}_{\delta_n}^{\otimes n}(P_n)\sigma^{\otimes n}\} \leq 2^{-n(\inf_{\rho \in \text{conv}(\mathcal{S}')} D(\rho \parallel \sigma) + d \cdot \log(1 - \delta_n) - \Theta(n, \varepsilon, d, \sigma))} \tag{34}$$

as well as, for every $\nu \in [0, 1)$ and $0 \leq A_n \leq \mathbb{1}^{\otimes n}$: if $\inf_{s^n \in \mathcal{S}^n} \text{tr}\{A_n \rho_{s^n}\} \geq 1 - \nu$, then

$$\text{tr}\{A_n \sigma^{\otimes n}\} \leq 2^{-n(\inf_{\rho \in \text{conv}(\mathcal{S}')} D(\rho \parallel \sigma) - \Gamma(n, \nu, d, \mathcal{N}_{\delta_n}(\sigma), \sqrt{n}) - c(\delta_n))}, \tag{35}$$

where $\tau \log(d) + h(\tau) + \tau \log(1/t_d) =: c(\tau, d, \sigma)$. Note that, for an arbitrary $\nu \in (0, 1)$, we have $\lim_{n \rightarrow \infty} \Gamma(n, \nu, d, \mathcal{N}_{\delta_n}(\sigma), \sqrt{n}) = 0$ and that also $\lim_{n \rightarrow \infty} c(\delta_n, d, \sigma) = 0$. This proves theorem 1 by replacing ε with $\varepsilon_n = \sqrt{1\alpha} \sqrt{\frac{1}{n} \log(\nu) + \frac{d^2 + \sqrt{n}}{n} \log(2n)}$.

Remark 3. By the linearity of the trace, this implies that we can distinguish the hypotheses $\text{conv}(\{\rho_{s^n}\}_{s^n \in \mathcal{S}^n})$ and $\sigma^{\otimes n}$ at the same rate.

The proof of theorem 4 reveals an interesting lemma, which is a generalization of the well-known concentration theorem for spectral estimation mentioned in our footnote 1. We state it here exclusively for sake of completeness.

Lemma 2. Let $\rho_{s^n} := \otimes_{i=1}^n \rho_{s_i}$ for a finite set $\{\rho_s\}_{s \in \mathcal{S}}$ of states. Let $\bar{\rho} := \sum_s \frac{1}{n} N(s|s^n) \rho_s$ and let $\lambda \in \mathbb{Y}_{d,n}$. Then

$$\text{tr}\{P_\lambda \rho_{s^n}\} \leq (2n)^{|\mathcal{S}| + d^2} 2^{-n(D(\bar{\lambda} \parallel \text{spec}(\bar{\rho}))}. \tag{36}$$

Our last result is of negative character.

Theorem 5. Let $n \in \mathbb{N}$, $\varepsilon \geq 0$ and a permutation invariant operator $A \in \mathcal{B}((\mathbb{C}^d)^{\otimes n})$, which is bounded by $0 \leq A_n \leq \mathbb{1}^{\otimes n}$, be given. Then

$$\min_{\rho \in \mathcal{S}(\mathbb{C}^d)} \text{tr}\{A_n \rho^{\otimes n}\} \geq 1 - \varepsilon \quad \Rightarrow \quad A_n \geq (1 - \varepsilon \cdot (2dn)^{4d^2}) \mathbb{1}^{\otimes n} \tag{37}$$

and, by applying this result to $(\mathbb{1}^{\otimes n} - A)$ instead of A :

$$\max_{\rho \in \mathcal{S}(\mathbb{C}^d)} \text{tr}\{A \rho^{\otimes n}\} \leq \varepsilon \quad \Rightarrow \quad A_n \leq \varepsilon \cdot (2dn)^{4d^2} \mathbb{1}^{\otimes n}. \tag{38}$$

Remark 4. A look at the proof of this theorem reveals that the decomposition $V_\lambda = \oplus_f V_{f,\lambda}$ is still not sufficiently fine for proving the theorem, indicating that there is some more relevant information to be gained by using POVMs that employ projections onto irreducible subspaces rather than the (generally reducible) ones that we employ. An even stronger method of types is thus still a possibility.

An operational implication of theorem 5's result is that any such sequence $((A_n, \mathbb{1}^{\otimes n} - A_n))_{n \in \mathbb{N}}$ of POVMs is useless for distinguishing between separable states and entangled states on $(\mathbb{C}^d)^{\otimes n}$, for large values of n : in the light of our theorem 4, and since $\mathcal{S}(\mathbb{C}^d) = \text{conv}(\mathcal{S}(\mathbb{C}^d))$, we see that any measurement scheme that successfully distinguishes between the hypotheses 'some fixed entangled state' versus 'any separable state' has a probability of successfully detecting the second hypothesis converging to one only polynomially fast, or it cannot be permutation invariant.

We arrive at our two main results by exploiting the simple observation that every frequency typical subspace V_f carries a representation of the symmetric group S_n and can therefore be decomposed into irreducible subspaces of S_n .

5. Proofs

Proof of theorem 2. This proof is split into several subsections. We start with the error exponent.

Proof that we have the correct error exponent in theorem 2. For a projection $P_{f,\lambda}$ we have, including the case that $t_{d-k}, \dots, t_d = 0$ for some $k > 0$ through the convention $2^{-\infty} = 0$ and the case that $\dim(F_\lambda) > 0$ but $\text{tr}\{P_{f,\lambda}\} = 0$ that can occur if V_f does not carry any of the representations corresponding to λ ,

$$\text{tr}\{P_{f,\lambda}\sigma^{\otimes n}\} \leq m_{\lambda,n} \dim(F_\lambda) 2^{n \sum_{i=1}^d \frac{1}{n} f_i \log(t_i)} \tag{39}$$

$$\leq m_{\lambda,n} 2^{n(H(\bar{\lambda}) + \sum_{i=1}^d \frac{1}{n} f_i \log t_i)}. \tag{40}$$

If, for some $s \in \mathbf{S}$, both $\|\bar{\lambda} - r_s\| \leq \varepsilon$ and $\|f - \tilde{r}_s\| \leq \varepsilon$, then equation (39) leads to

$$\text{tr}\{P_{f,\lambda}\sigma^{\otimes n}\} \leq m_{\lambda,n} 2^{n(H(r_s) + \varepsilon|\log(\varepsilon/d)| + \sum_{i=1}^d \tilde{r}_s(i) \log t_i + d\varepsilon \cdot \max_i |\log t_i|)}. \tag{41}$$

But for an orthonormal eigenbasis $\{e_i^s\}_{i=1}^d$ of ρ_s , we have $\tilde{r}_s(i) = \sum_j |\langle \tilde{e}_i, e_j^s \rangle|^2 r_s(j)$ and so

$$H(r) + \sum_{i=1}^d \tilde{r}_s(i) \log t_i = -D(\rho_s \| \sigma), \tag{42}$$

and for the projection P_n this means that

$$\text{tr}\{P_n \sigma^{\otimes n}\} = \sum_{(f,\lambda) \in \Lambda_\varepsilon} \text{tr}\{P_{f,\lambda}\sigma^{\otimes n}\} \tag{43}$$

$$\leq (2n)^{d^2} \max_{(f,\lambda) \in \Lambda_\varepsilon} \text{tr}\{P_{f,\lambda}\sigma^{\otimes n}\} \tag{44}$$

$$\leq (2n)^{d^2} \sup_{s \in \mathbf{S}} 2^{-n(D(\rho_s \| \sigma) - \varepsilon|\log(\varepsilon/d)| - d\varepsilon \cdot \max_i |\log t_i|)} \tag{45}$$

$$= 2^{-n(\inf_{s \in \mathbf{S}} D(\rho_s \| \sigma) - \frac{d^2}{n} \log(2n) - \varepsilon|\log(\varepsilon/d)| - d\varepsilon \cdot \max_i |\log t_i|)} \tag{46}$$

$$= 2^{-n(\inf_{s \in \mathbf{S}} D(\rho_s \| \sigma) - \Theta(n, \varepsilon, d, \sigma))}, \tag{47}$$

which is what we wanted to show.

Proof that we can identify every state in our given set with high probability. For every $s \in \mathbf{S}$, define the projections $P_{n,s} := \sum_{f: \|\tilde{f} - \tilde{r}_s\| \leq \varepsilon} \sum_{\lambda: \|\bar{\lambda} - r_s\| \leq \varepsilon} P_{f,\lambda}$. These satisfy the lower bound

$$\forall s \in \mathbf{S}, \quad P_n \geq P_{n,s}. \tag{48}$$

Another inequality we will need is an upper bound that is valid for all $P_{f,\lambda}$ satisfying $\text{tr}\{P_{f,\lambda} P_{n,s}\} = 0$. It generally holds that $P_{f,\lambda} \leq \sum_\lambda P_{f,\lambda} =: P_f$ and $P_{f,\lambda} \leq \sum_f P_{f,\lambda} =: P_\lambda$, and thus by the results mentioned in our footnote 1 and the basic estimate lemma 2.6 in [19] followed by Pinsker's inequality, we get the upper bound

$$\text{tr}\{\rho_s^{\otimes n} P_{f,\lambda}\} \leq \min \{ \text{tr}\{\rho_s^{\otimes n} P_f\}, \text{tr}\{\rho_s^{\otimes n} P_\lambda\} \} \tag{49}$$

$$\leq (2n)^{d^2} \min \{ 2^{-nD(\bar{\lambda} \| r_s)}, 2^{-nD(\tilde{f} \| \tilde{r}_s)} \} \tag{50}$$

$$\leq (2n)^{d^2} 2^{-n\alpha\varepsilon^2}. \tag{51}$$

Set $X_s := \{(f, \lambda) : \|\bar{f} - \tilde{r}_s\| > \varepsilon \wedge \|\bar{\lambda} - r_s\| > \varepsilon\}$. From the definition of our basic object it can be seen that the inequality $\sum_f \sum_\lambda P_{f,\lambda} = \mathbb{1}^{\otimes n}$ holds, so for an arbitrary $s \in \mathbf{S}$ we have

$$1 = \text{tr} \left\{ \rho_s^{\otimes n} \sum_f \sum_\lambda P_{f,\lambda} \right\} \tag{52}$$

$$= \text{tr} \{ \rho_s^{\otimes n} P_{n,s} \} + \text{tr} \{ \rho_s^{\otimes n} (\mathbb{1}_{\mathbb{C}^d} - P_{n,s}) \} \tag{53}$$

$$\leq \text{tr} \{ \rho_s^{\otimes n} P_{n,s} \} + (2n)^{d^2} \max_{(f,\lambda) \in X_s} \text{tr} \{ \rho_s^{\otimes n} P_{f,\lambda} \} \tag{54}$$

$$\leq \text{tr} \{ \rho_s^{\otimes n} P_{n,s} \} + (2n)^{2d^2} 2^{-n\alpha\varepsilon^2} \tag{55}$$

$$\leq \text{tr} \{ \rho_s^{\otimes n} P_n \} + (2n)^{2d^2} 2^{-n\alpha\varepsilon^2}. \tag{56}$$

It follows

$$\inf_{s \in \mathbf{S}} \text{tr} \{ \rho_s^{\otimes n} P_n \} \geq 1 - 2^{-n(\alpha\varepsilon^2 - \frac{2d^2}{n} \log(2n))}. \tag{57}$$

Therefore,

$$\lim_{n \rightarrow \infty} \inf_{s \in \mathbf{S}} \text{tr} \{ P_n \rho_s^{\otimes n} \} = 1, \tag{58}$$

as required. By the linearity of the trace, the results immediately imply that we can also (asymptotically) distinguish the sequence $(\text{conv}(\{\rho_s^{\otimes n}\}_{s \in \mathbf{S}}))_{n \in \mathbb{N}}$ of sets from the sequence $(\sigma^{\otimes n})_{n \in \mathbb{N}}$.

Proof of the lower bound on the error exponent in theorem 2. Let an operator $0 \leq A \leq \mathbb{1}^{\otimes n}$ be given that satisfies

$$\inf_{s \in \mathbf{S}} \text{tr} \{ A \rho_s^{\otimes n} \} \geq 1 - \nu \tag{59}$$

for some $\nu \in (0, 1)$. Note that we can without loss of generality assume that A is permutation-invariant, since permuting an A that is not invariant does change neither $\text{tr}\{A \rho^{\otimes n}\}$ nor $\text{tr}\{A \sigma^{\otimes n}\}$. But then by Schur–Weyl duality we can write

$$A = \sum_\lambda A_\lambda, \tag{60}$$

where $0 \leq A_\lambda \leq c_\lambda P_\lambda$ for some set of real numbers c_λ . This leads us to

$$\text{tr} \{ \sigma^{\otimes n} A_\lambda \} = \sum_{\lambda, f, j} 2^{n \sum_i \tilde{f}(i) \log t_i} \text{tr} \{ P_{f,\lambda,j} A_\lambda P_{f,\lambda,j} \}, \tag{61}$$

where $P_{f,\lambda,j}$ are any set of mutually *orthogonal* and *irreducible* projections such that $P_{f,\lambda} = \sum_j P_{f,\lambda,j}$ for all (f, λ) . On the other hand, by lemma 9 in [24] we get

$$\sum_{f,\lambda,j} P_{f,\lambda,j} A P_{f,\lambda,j} \geq (2n)^{-d^2} A, \tag{62}$$

and it follows

$$1 - \nu \leq (2n)^{d^2} \sum_{f,\lambda,j} \text{tr} \{ P_{f,\lambda,j} A P_{f,\lambda,j} \rho^{\otimes n} \}. \tag{63}$$

It is clear that $P_{f,\lambda,j}AP_{f,\lambda,j} = c_{f,\lambda,j}P_{f,\lambda,j}$ for every triple (f, λ, j) and a suitable choice of coefficients $0 \leq c_{f,\lambda,j} \leq 1$ by the permutation-invariance of A . Therefore there is at least one (f, λ, j) such that $\|f - \tilde{r}\| \leq n^{-1/4}$, $\|\bar{\lambda} - r\| \leq n^{-1/4}$ and

$$c_{f,\lambda,j} \geq (2n)^{-2d^2} (1 - \nu - 2^{-\alpha\sqrt{n}}). \tag{64}$$

But this implies that for this triple (f, λ, j) we have (and at this point one sees again that it is crucial that we have defined the V_f using the eigenbasis of σ , since this ensures that $\sigma^{\otimes n}$ and every one of the $P_{f,\lambda,j}$ commute)

$$\text{tr}\{\sigma^{\otimes n}A\} \geq \text{tr}\{\sigma^{\otimes n}A_\lambda\} \tag{65}$$

$$= \sum_{f',i} \text{tr}\{\sigma^{\otimes n}P_{f',i}A_\lambda P_{f',i}\} \tag{66}$$

$$\geq 2^{n \sum_i \bar{f}(i) \log t_i} \text{tr}\{P_{f,\lambda,j}A_\lambda P_{f,\lambda,j}\} \tag{67}$$

$$= 2^{n \sum_i \bar{f}(i) \log t_i} \text{tr}\{P_{f,\lambda,j}\}c_{f,\lambda,j} \tag{68}$$

$$\geq 2^{n \sum_i \bar{f}(i) \log t_i} \dim(F_\lambda) \frac{1 - \nu - 2^{-\alpha\sqrt{n}}}{(2n)^{2d^2}} \tag{69}$$

$$\geq 2^{n(\sum_i \bar{f}(i) \log(t_i) - H(\bar{\lambda}) - \frac{2d^6}{n} \log(2n))} \frac{1 - \nu - 2^{-\alpha\sqrt{n}}}{(2n)^{2d^2}} \tag{70}$$

$$\geq 2^{-n(D(\rho\|\sigma) - \Theta(n, n^{-\frac{1}{4}}, d) - \frac{2d^6}{n} \log(2n) + \frac{1}{n} \log\left(\frac{1 - \nu - 2^{-\alpha\sqrt{n}}}{(2n)^{2d^2}}\right))}, \tag{71}$$

so the function

$$\Theta'(n, \nu, d) := \Theta(n, n^{-\frac{1}{4}}, d) - \frac{2d^6}{n} \log(2n) + \frac{1}{n} \log\left(\frac{1 - \nu - 2^{-\alpha\sqrt{n}}}{(2n)^{2d^2}}\right) \tag{72}$$

does the job. □

Proof of theorem 3. Let us first state some known facts about Kostka numbers. It holds that $K_{f,\lambda} > 0 \Leftrightarrow f < \lambda$. But $K_{f,\lambda}$ is just the number of ways to fill the tableau λ with numbers from $[d]$ such that the numbers in the filling are weakly increasing in each row, read from left to right, and are strictly increasing along the columns (read from top to bottom). Thus $K_{f,\lambda} > 0 \Leftrightarrow \text{tr}\{P_{f,\lambda}\} > 0$. There is actually another important equivalence that we shall use: $f < \lambda \Leftrightarrow f = D\lambda$ for some doubly stochastic matrix D .

Now assume $K_{f,\lambda} > 0$ holds. Thus $f = D\lambda$ for some doubly stochastic matrix D . In this case we may define a state ρ by the following procedure. Pick any basis $\{e_i\}_{i=1}^d$. Choose a unitary matrix $U = \sum_{i,j} u_{ij}|e_i\rangle\langle e_j|$ such that for the matrix coefficients of D it holds that $D_{ij} = |u_{ij}|^2$ for all $i, j \in [d]$. This can be done, thanks to Horn's lemma [28]. Define $\rho := \sum_i \bar{\lambda}_i |e_i\rangle\langle e_i|$, then $\langle e_i, U\rho U^\dagger e_i \rangle = f(i)$ for all $i \in [d]$, and this means that the pinching of ρ to the basis $\{U^\dagger e_i\}_{i=1}^d$ satisfies our requirements.

Now take any state ρ with spectrum r_ρ and pinching \tilde{r}_ρ in some (not exactly specified) basis. If $\rho = \frac{1}{d}\mathbb{1}$, there is nothing to prove, since every pinching then satisfies $\tilde{r}_\rho = r_\rho$, and obviously choosing $D = Id$ is consistent with the elementary fact that $K_{nr_\rho, nr_\rho} > 0$ for every n such that $n/d \in \mathbb{N}$.

Thus, $\rho \neq \frac{1}{d}\mathbb{1}$. Choosing $\sigma = \frac{1}{d}\mathbb{1}$ it follows that $D(\rho\|\sigma) > 0$, and using our projections P_n we see from equation (57) that there is $N \in \mathbb{N}$ such that for all $n \geq N$ there is a projection $P_{f,\lambda} \neq 0$ that has the property $\|\tilde{f} - \tilde{r}_\rho\| \leq n^{-\frac{1}{4}}$ and $\|\tilde{\lambda} - r_\rho\| \leq n^{-\frac{1}{4}}$, proving our claim. \square

Proof of theorem 4. We will first show the statements in the case that \mathfrak{S}' is finite, and then apply them to the case of an infinite set \mathfrak{S}' . The issues arising in the latter setting are mainly due to the ‘roundness’ of the set of states. It could possibly happen that \mathfrak{S}' contains parts of the boundary of the set of $\mathcal{S}(\mathbb{C}^d)$, and it can then (thinking of the Bloch sphere representation is helpful here) be impossible to include \mathfrak{S}' into the convex hull of some finite set that lies entirely within the set of states itself.

Robustification, part I—finite \mathbf{S} . Let a state $\rho_{\mathfrak{S}^n}$ be given, and let \mathfrak{S}^n have type $N : \mathbf{S} \rightarrow \mathbb{N}$ (meaning that the short-hand $N(\cdot) = N(\cdot|s^n)$ is valid). Let $p \in \mathfrak{P}(\mathbf{S})$ be defined by $p(s) := \frac{1}{n}N(s)$. It then holds (see [19], the proof of lemma 2.3) that $p^{\otimes n}(T_N) \geq (2n)^{-|\mathbf{S}|}$. Since our measurement is permutation-invariant, it follows that

$$\text{tr} \left\{ (\mathbb{1} - P_n) \left(\sum_{s \in \mathbf{S}} p(s)\rho_s \right)^{\otimes n} \right\} = \text{tr} \left\{ (\mathbb{1} - P_n) \sum_{s^n \in \mathfrak{S}^n} p^{\otimes n}(s^n)\rho_{s^n} \right\} \tag{73}$$

$$\geq \text{tr} \left\{ (\mathbb{1} - P_n) \sum_{s^n \in T_N} p^{\otimes n}(s^n)\rho_{s^n} \right\} \tag{74}$$

$$= \text{tr} \left\{ (\mathbb{1} - P_n) \sum_{s^n \in T_N} p^{\otimes n}(s^n)\rho_{\mathfrak{S}^n} \right\} \tag{75}$$

$$= p^{\otimes n}(T_N)\text{tr}\{(\mathbb{1} - P_n)\rho_{\mathfrak{S}^n}\} \tag{76}$$

$$\geq (2n)^{-|\mathbf{S}|}\text{tr}\{(\mathbb{1} - P_n)\rho_{\mathfrak{S}^n}\}, \tag{77}$$

implying, via equation (57) and our choice of P_n , that

$$\text{tr}\{P_n\rho_{\mathfrak{S}^n}\} = 1 - \text{tr}\{(\mathbb{1} - P_n)\rho_{\mathfrak{S}^n}\} \tag{78}$$

$$\geq 1 - (2n)^{|\mathbf{S}|}\text{tr} \left\{ (\mathbb{1} - P_n) \left(\sum_{s \in \mathbf{S}} p(s)\rho_s \right)^{\otimes n} \right\} \tag{79}$$

$$\geq 1 - (2n)^{|\mathbf{S}|}2^{-n\left(\alpha\varepsilon^2 + \frac{2d^2}{n}\log(2n)\right)} \tag{80}$$

$$\geq 1 - 2^{-n\left(\alpha\varepsilon^2 + \frac{2d^2+|\mathbf{S}|}{n}\log(2n)\right)}. \tag{81}$$

By the linearity of the trace, this immediately implies that we can distinguish the sequence $(\text{conv}(\{\rho_{s^n}\}_{s^n \in \mathfrak{S}^n}))_{n \in \mathbb{N}}$ of sets from the sequence $(\sigma^{\otimes n})_{n \in \mathbb{N}}$.

We still have to show that we have the right error exponent, but this follows immediately from the Sanov case by noting that for arbitrary $s^n \in \mathfrak{S}^n$ and the type $N(\cdot) := N(\cdot|s^n)$ we have by lemma 2.3 in [19]

$$\text{tr}\{P_n\rho_{s^n}\} \leq (2n)^{|\mathbf{S}|}\text{tr} \left\{ P_n \left(\sum_{s \in \mathbf{S}} \bar{N}(s)\rho_s \right)^{\otimes n} \right\}. \tag{82}$$

Proof of the converse part for finite $|\mathbf{S}|$. Let $\text{tr}\{A\rho_{s^n}\} \geq 1 - \nu$ for all $s^n \in \mathbf{S}^n$. Like before, we can without loss of generality assume that A is permutation-invariant. Then again by lemma 5 in [24], we get

$$A \leq (2n)^{d^2} \sum_{f,\lambda,j} c_{f,\lambda,j} P_{f,\lambda,j}, \tag{83}$$

where $P_f := \sum_{\lambda} P_{f,\lambda}$, $P_{\lambda} := \sum_f P_{f,\lambda}$ and $P_f P_{\lambda} = P_{\lambda} P_f$ holds, and the index j refers to any decomposition $V_{f,\lambda} = \oplus_{\lambda,j} V_{f,\lambda,j}$ into *irreducible* components. Obviously, $P_{f,\lambda,j}$ then denote the orthogonal projections onto the $V_{f,\lambda,j}$.

Let us pick $p \in \mathfrak{P}(\mathbf{S})$ and an $s^n \in \mathbf{S}^n$ having a type abbreviated by $N(\cdot) = N(\cdot|s^n)$. We may additionally assume that N satisfies $\|\bar{N} - p\| \leq \delta_n$ (where $\delta_n = 2|\mathbf{S}|/n$). Then assume that a $\lambda \in \mathbb{Y}_{d,n}$ satisfies $\|\bar{\lambda} - \text{spec}(\bar{\rho})\| > \delta > 0$ for some δ and the state $\bar{\rho} := \sum_s p(s)\rho_s$. For such λ it follows from [19], lemma 2.3, that

$$\text{tr}\{P_{\lambda}\rho_{s^n}\} = \frac{1}{|T_N|} \sum_{s^n \in T_N} \text{tr}\{P_{\lambda}\rho_{s^n}\} \tag{84}$$

$$\leq (2n)^{|\mathbf{S}|} \bar{N}^{\otimes n}(T_N) \sum_{s^n \in T_N} \text{tr}\{P_{\lambda}\rho_{s^n}\} \tag{85}$$

$$\leq (2n)^{|\mathbf{S}|} \sum_{s^n \in \mathbf{S}^n} \bar{N}^{\otimes n}(s^n) \text{tr}\{P_{\lambda}\rho_{s^n}\} \tag{86}$$

$$= (2n)^{|\mathbf{S}|} \text{tr} \left\{ P_{\lambda} \left(\sum_s \bar{N}(s)\rho_s \right)^{\otimes n} \right\} \tag{87}$$

$$\leq (2n)^{|\mathbf{S}|} (2n)^{d^2} 2^{-nD(\bar{\lambda}, \|\text{spec}(\sum_s \bar{N}(s)\rho_s))} \tag{88}$$

$$\leq (2n)^{|\mathbf{S}|+d^2} 2^{-n\alpha \|\bar{\lambda} - \text{spec}(\sum_s \bar{N}(s)\rho_s)\|^2} \tag{89}$$

$$\leq (2n)^{|\mathbf{S}|+d^2} 2^{-n\alpha (\|\bar{\lambda} - \text{spec}(\bar{\rho})\| - \|\text{spec}(\bar{\rho}) - \text{spec}(\sum_s \bar{N}(s)\rho_s)\|)^2} \tag{90}$$

$$\leq (2n)^{|\mathbf{S}|+d^2} 2^{-n\alpha (\|\bar{\lambda} - \text{spec}(\bar{\rho})\| - \delta_n)^2} \tag{91}$$

$$\leq (2n)^{|\mathbf{S}|+d^2} 2^{-n\alpha (\|\bar{\lambda} - \text{spec}(\bar{\rho})\|^2 - 2\delta_n)} \tag{92}$$

$$\leq (2n)^{|\mathbf{S}|+d^2} 2^{-n\alpha (\delta^2 - 2\delta_n)}, \tag{93}$$

where the third inequality counted from below is due to inequality (1) in [5]. In the same way, we get that, for all frequencies f satisfying $\|\bar{f} - \tilde{r}_{\bar{\rho}}\| > \delta$, we have the following inequality:

$$\text{tr}\{P_f \rho_{s^n}\} \leq (2n)^{|\mathbf{S}|+d^2} 2^{-n\alpha (\delta^2 - 2\delta_n)}. \tag{94}$$

We use these results to get (using the abbreviation $\bar{\rho} := \sum_s p(s)\rho_s$) the following:

$$1 - \nu \leq (2n)^{d^2} \sum_{f,\lambda,j} c_{f,\lambda,j} \text{tr}\{P_{f,\lambda,j}\rho_{s^n}\} \tag{95}$$

$$\leq (2n)^{d^2} \sum_{f,\lambda,j} c_{f,\lambda,j} \text{tr}\{P_{f,\lambda,j}\rho_{s^n}\} \tag{96}$$

$$\leq (2n)^{d^2} \sum_{\|\bar{f}-\bar{r}_{\bar{\rho}}\|\leq\delta} \sum_{\|\bar{\lambda}-r_{\bar{\rho}}\|\leq\delta} c_{f,\lambda,j} \text{tr}\{P_{f,\lambda,j}\rho_{S^n}\} + (2n)^{|\mathbf{S}|+2d^2} 2^{-n\alpha(\delta^2-2\delta_n)} \quad (97)$$

$$\leq (2n)^{2d^2} \max\{c_{f,\lambda,j} : \|\bar{\lambda}-r_{\bar{\rho}}\|\leq\delta, \|\bar{f}-\bar{r}_{\bar{\rho}}\|\leq\delta\} + 2^{-n[\alpha(\delta^2-2\delta_n)-\frac{|\mathbf{S}|+2d^2}{n}\log(2n)]}, \quad (98)$$

and choosing $\delta = n^{-1/8}$ we get (as before) that there exists a triple (f, λ, j) such that $\|\bar{\lambda}-r_{\bar{\rho}}\|\leq n^{-1/8}$ and $\|\bar{f}-\bar{r}_{\bar{\rho}}\|\leq n^{-1/8}$ and at the same time

$$(1-\nu-2^{-n[\alpha(n^{-1/4}-4|\mathbf{S}|n^{-1})-\frac{|\mathbf{S}|-2d^2}{n}\log(2n)]})(2n)^{-2d^2} \leq c_{f,\lambda,j}. \quad (99)$$

Let us abbreviate this by writing instead that, for the quantity

$$\Gamma'(n, d, \nu, |\mathbf{S}|) := \frac{1}{n} \log[(1-\nu-2^{-n[\alpha(n^{-1/4}-4|\mathbf{S}|n^{-1})-\frac{|\mathbf{S}|-2d^2}{n}\log(2n)]})(2n)^{-2d^2}], \quad (100)$$

we have

$$c_{f,\lambda,j} \geq 2^{n\Gamma'(n,d,\nu,|\mathbf{S}|)}. \quad (101)$$

It is also important to note that $\lim_{n\rightarrow\infty} \Gamma'(n, d, \nu, |\mathbf{S}|) = 0$, if the other values remain fixed. This leads to

$$\text{tr}\{A\sigma^{\otimes n}\} \geq c_{f,\lambda,j} \text{tr}\{P_{f,\lambda,j}\sigma^{\otimes n}\} \quad (102)$$

$$\geq 2^{n\Gamma'(n,d,|\mathbf{S}|)} 2^{n(H(\bar{\lambda})-\frac{2d^6}{n}\log(2n))} 2^{n\sum_i \bar{f}(i)\log t_i} \quad (103)$$

$$\geq 2^{-n(D(\bar{\rho}\|\sigma)+\Theta(n,n^{-\frac{1}{8}},d,\sigma)-\Gamma'(n,d,\nu,|\mathbf{S}|)+\frac{2d^6}{n}\log(2n))} \quad (104)$$

$$= 2^{-nD(\bar{\rho}\|\sigma)+\Gamma(n,\nu,d,\sigma,|\mathbf{S}|)}, \quad (105)$$

with the obvious definition of the function Γ . Note that $\lim_{n\rightarrow\infty} \Gamma(n, \nu, d, \sigma, |\mathbf{S}|) = 0$ for all $\nu \in (0, 1)$. But the above estimate holds for all $\bar{\rho} \in \text{conv}(\mathfrak{S}')$, so

$$\text{tr}\{A\sigma^{\otimes n}\} \geq 2^{-n(\inf_{\rho \in \text{conv}(\mathfrak{S}')} D(\rho\|\sigma)-\Gamma(n,\nu,d,\sigma,|\mathbf{S}|))}. \quad (106)$$

Robustification, part II—infinite S. We will approximate the set \mathbf{S} by finite sets first, to which we then apply the previous result. We proceed as follows. First, we drag the set \mathfrak{S}' a bit into the direction of the center of $\mathcal{S}(\mathbb{C}^d)$ by applying an appropriate cptp map. The result will be that the so-modified set \mathfrak{S}'' has a positive set distance from the boundary of $\mathcal{S}(\mathbb{C}^d)$. We can then find a finite set \mathfrak{S}''' of states such that $\mathfrak{S}'' \subset \text{conv}(\mathfrak{S}''')$ holds. The adjoint of our cptp map applied to our invariant projections then defines our measurement. Unfortunately, this means that our measurement operators in this scenario are no longer extremal.

Let us get started.

Without diving deeper into issues concerning distances between sets at this point, it is clear that (for the convex set $\mathfrak{S} := \text{conv}(\mathfrak{S}')$) the statement $\sigma \notin \mathfrak{S}$ implies that there is a small δ satisfying $1 > \delta > 0$ such that the channel

$$\mathcal{N}_\delta(\cdot) := (1-\delta)Id(\cdot) + \delta \frac{1}{d} \mathbb{1} \quad (107)$$

has the property that $\sigma \notin \mathcal{N}_\delta(\mathfrak{S})$. Since the case $\sigma \in \mathfrak{S}$ is trivial, we may assume that $\sigma \notin \mathfrak{S}$ without loss of generality. Define $\mathfrak{S}'' := \mathcal{N}_\delta(\mathfrak{S})$. Now take any finite set $\mathfrak{S}''' = \{\hat{\rho}_s\}_{s \in \mathfrak{S}''}$ such that $\mathfrak{S}'' \subset \text{conv}(\mathfrak{S}''')$. Then, applying the result from the previous proof to our new set $\text{conv}(\mathfrak{S}''')$, we see that

$$\text{tr}\{P_n \rho'_{S^n}\} \geq 1 - 2^{-n(\alpha\epsilon^2 + \frac{2d^2+|\mathfrak{S}'''|}{n}\log(2n))} \quad (108)$$

holds for all ρ'_{s^n} for which $\rho'_{s_i} \in \text{conv}(\mathfrak{S}''')$ for all $i = 1, \dots, n$. But for the transpose channel $\mathcal{N}_\delta^\dagger$ of \mathcal{N}_δ , this implies that for all $s^n \in \mathbf{S}^n$ we have

$$\text{tr}\{\mathcal{N}_\delta^{\dagger \otimes n}(P_n)\rho_{s^n}\} \geq 1 - 2^{-n(\alpha\epsilon^2 + \frac{d^2 + |\mathbf{S}'''|}{n} \log(2n))}. \tag{109}$$

Since $0 \leq \mathcal{N}_\delta^{\dagger \otimes n}(P_n) \leq \mathbb{1}^{\otimes n}$ holds, we have succeeded in constructing a measurement that correctly identifies the AVQS \mathfrak{S}' . The next step naturally is to make δ very small, and to hope that we then get closer and closer to the optimal exponent. This will of course come at a price: the lower bound (108) is dependent on the size \mathbf{S}''' of the number of extremal points in our finite approximation of \mathfrak{S}' —and this number increases with δ . We shall now quantify this.

Consider the supporting hyperplane of $\mathfrak{S}' \cup \{\frac{1}{d}\mathbb{1}\}$ as a real vector space W that contains all the sets $\mathfrak{S}, \mathfrak{S}', \mathfrak{S}''$. All operators in $a \in W$ obey $\text{tr}\{a\} = 1$. Obviously, this vector space does contain matrices that are not in $\mathcal{S}(\mathbb{C}^d)$ —they have negative eigenvalues. We want to construct a finite approximation \mathfrak{S}''' to \mathfrak{S}'' such that $\mathfrak{S}'' \subset \text{conv}(\mathfrak{S}''') \subset \mathcal{S}(\mathbb{C}^d)$.

On W , we may still use the one-norm $\|\cdot\|$ as a norm. The intersection $B := \text{rebd}\mathcal{S}(\mathbb{C}^d) \cap W$ satisfies $\mathfrak{S}'' \subset \text{conv}(B)$, and it is thus our goal to construct an approximation satisfying $\mathfrak{S}'' \subset \text{conv}(\mathfrak{S}''') \subset \text{conv}(B)$. On W , a δ -net in 1-norm of cardinality no more than $N(\delta) \leq (2/\delta)^{2d^2}$ can be found via the volume bound from [31] (lemma 2.6) in its application to quantum states (see e.g. [6], lemma 5.1, and note that quantum states are just special instances of quantum channels). We additionally need to show that the blow-up $(\mathfrak{S}'')_\epsilon$ is contained in $\text{conv}(B)$ for small enough $\epsilon > 0$. This is done by taking any normalized vector $x \in \mathbb{C}^d$ and computing, for some $a \in W$ satisfying $\|a - \mathcal{N}_\delta(\rho_s)\| \leq \epsilon$,

$$\langle x, ax \rangle = \langle x, (a - \mathcal{N}_\delta(\rho_s))x \rangle + \langle x, \mathcal{N}_\delta(\rho_s)x \rangle \tag{110}$$

$$\geq \langle x, (a - \mathcal{N}_\delta(\rho_s))x \rangle + \delta/2 \tag{111}$$

$$\geq \delta/2 - \epsilon, \tag{112}$$

and for $\epsilon \leq \delta/2$ this is larger than or equal to zero. So, applying \mathcal{N}_δ guarantees us that $(\mathcal{N}_\delta(\mathfrak{S}'))_{\delta/2} \subset \text{conv}(B) \subset \mathcal{S}(\mathbb{C}^d)$.

It can be read off from [38], theorems 3.1.6 and 1.8.5 and the above cardinality bounds for δ -nets that $|\mathbf{S}''| \leq (12/\delta)^{2d^2}$ can be chosen. Now replace δ by $\delta_n = 12n^{-1/(4d^2)}$, then $|\mathbf{S}''| \leq \sqrt{n}$. Thus,

$$\text{tr}\{\mathcal{N}_{\delta_n}^{\dagger \otimes n}(P_n)\rho_{s^n}\} \geq 1 - 2^{-n(\alpha\epsilon^2 + \frac{d^2 + \sqrt{n}}{n} \log(2n))} \quad \forall \rho_{s^n} \in \mathfrak{S}^{\otimes n}. \tag{113}$$

At the same time, looking back to our equations (39) to (47), we see that the following is valid:

$$\text{tr}\{\mathcal{N}_\delta^{\dagger \otimes n}(P_n)\sigma^{\otimes n}\} = \text{tr}\{P_n \mathcal{N}_\delta^{\otimes n}(\sigma^{\otimes n})\} \tag{114}$$

$$\leq 2^{-n(\inf_{\rho \in \mathfrak{S}} D(\rho \| \mathcal{N}_\delta(\sigma)) - \Theta(n, \epsilon, d, \mathcal{N}_{\delta_n}(\sigma))}. \tag{115}$$

It still holds that $\lim_{n \rightarrow \infty} \Theta(n, \epsilon, d, \mathcal{N}_{\delta_n}(\sigma)) = 0$, but by monotonicity of the relative entropy it is not yet clear that this is in general the optimal exponent. By assumption, $\inf_{\rho \in \mathfrak{S}} D(\rho \| \sigma) < \infty$. Then also $\inf_{\rho \in \mathfrak{S}} D(\rho \| \mathcal{N}_{\delta_n}(\sigma)) < \infty$ so that for every $\rho \in \mathfrak{S}$ and for $\delta_n < t_d$, we also have

$$D(\rho \| \mathcal{N}_{\delta_n}(\sigma)) = D(\rho \| \sigma) - \text{tr}\{\rho(\log(\mathcal{N}_{\delta_n}(\sigma)) - \log(\sigma))\} \tag{116}$$

$$\geq D(\rho \| \sigma) - d \cdot \max_i \log\left(\frac{t_i}{(1 - \delta_n)t_i + \delta_n/2}\right) \tag{117}$$

$$\geq D(\rho \| \sigma) - d \cdot \log\left(\frac{t_1}{(1 - \delta_n)t_1 + \delta_n/2}\right) \tag{118}$$

$$\geq D(\rho\|\sigma) - d \cdot \log\left(\frac{t_1}{(1 - \delta_n)t_1}\right) \tag{119}$$

$$= D(\rho\|\sigma) + d \cdot \log(1 - \delta_n). \tag{120}$$

Clearly, this proves

$$\text{tr}\{\mathcal{N}_{\delta_n}^{\dagger\otimes n}(P_n)\sigma^{\otimes n}\} \leq 2^{-n(\inf_{\rho \in \text{conv}(\mathfrak{S})} D(\rho\|\sigma) + d \cdot \log(1 - \delta_n) - \Theta(n, d, \varepsilon, \mathcal{N}_{\delta_n}(\sigma)))}. \tag{121}$$

Proof of the lower bound on the error exponent in theorem 4 for infinite |S|. Luckily, in this converse part of the proof we do not have to approximate \mathfrak{S} from the outside—an approximation from the inside is enough. We will need the Fannes–Audenaert inequality, which yields the following bound:

$$|D(\rho\|\sigma) - D(\rho'\|\sigma)| \leq \tau \log(d) + h(\tau) + \tau \log(1/t_d) =: c(\tau), \tag{122}$$

where $\tau := \frac{1}{2}\|\rho - \rho'\|$. Then, as before, we approximate an infinite set $\text{conv}(\mathfrak{S})$ by a sequence $\text{conv}(\mathfrak{S}_n)_{n \in \mathbb{N}}$ of convex sets, each $\text{conv}(\mathfrak{S}_n)$ having finitely many extremal points $\{\rho_x\}^{(n)}_{x \in X_n}$, where $|X_n| \leq \sqrt{n}$, and for each $\rho \in \text{conv}(\mathfrak{S})$ and $n \in \mathbb{N}$ there is a $\rho' \in \text{conv}(\mathfrak{S}_n)$ such that $\|\rho - \rho'\| \leq 12n^{-1/4d^2}$. Then, by playing everything back to the finite case and using the scaling of $|X_n|$, we get

$$\text{tr}\{A\sigma^{\otimes n}\} \geq 2^{-n(\inf_{\rho \in \text{conv}(\mathfrak{S})} D(\rho\|\sigma) + c(12n^{-1/4d^2}) + \Gamma(n, \varepsilon, d, \sigma, \sqrt{n}))}. \tag{123}$$

This proves our claim, since $\lim_{n \rightarrow \infty} \Gamma'(n, \varepsilon, d, \sqrt{n}) = 0$ for all $\varepsilon \in (0, 1)$. □

Proof of our no-go-result, theorem 5. Let a permutation-invariant operator $A \in \mathcal{B}((\mathbb{C}^d)^{\otimes n})$ satisfy the inequalities $0 \leq A \leq \mathbb{1}$ and

$$1 - \varepsilon \leq \text{tr}\{A\rho^{\otimes n}\} \quad \forall \rho \in \mathcal{S}(\mathbb{C}^d) \tag{124}$$

for some $\varepsilon > 0$. Then due to the Schur–Weyl duality, $\mathbb{1} - A$ can be written $\mathbb{1} - A = \sum_{\lambda} A_{\lambda}$ with each A_{λ} satisfying $P_{\lambda}c_{\lambda} \geq A_{\lambda} \geq 0$ for some $1 \geq c_{\lambda} \geq 0$, where P_{λ} is the projection onto the isotypical subspace corresponding to λ . It follows that if we average an A_{λ} over the unitary group, we get for every ρ that

$$\text{tr}\left\{\int d_U U^{\otimes n} A_{\lambda} U^{\dagger \otimes n} \rho^{\otimes n}\right\} \leq \int d_U \text{tr}\{U^{\otimes n} (\mathbb{1} - A) U^{\dagger \otimes n} \rho^{\otimes n}\} \leq \int d_U \varepsilon = \varepsilon. \tag{125}$$

Let λ be fixed for the moment. Let the invariant subspace V_{λ} have a decomposition into irreducible components of S_n as $V_{\lambda} = \bigoplus_i V_i$. The operator A_{λ} can then, due to Schur–Weyl duality, be written as

$$A_{\lambda} = \sum_{i,j=1}^{m_{n,\lambda}} c_{ij} Y_{ij}, \tag{126}$$

for operators Y_{ij} such that for each pair $i \neq j$, the operator Y_{ij} commutes with the action of the permutation group and maps the irreducible representation V_j to V_i , and each $P_i := Y_{ii}$ is the orthogonal projection onto V_i . Moreover, $\text{tr}\{Y_{ij}\} = \delta(i, j) \dim(F_{\lambda})$. The numbers c_{ij} satisfy $c_{ii} \geq 0$ for all $i \in [m_{n,\lambda}]$ and $|c_{ij}| \leq \sqrt{|c_{ii}| \cdot |c_{jj}|}$, since $A_{\lambda} \geq 0$.

Now choose a state ρ with spectrum t satisfying $t = \lambda$, and observe that $\int d_U (U\rho U^{\dagger})^{\otimes n} = \sum_{\lambda} u_{\lambda} P_{\lambda}$ for an appropriate number $0 \leq u_{\lambda} \leq 1$, so that for every $i \in [m_{\lambda,n}]$:

$$\varepsilon \geq \text{tr}\left\{A_{\lambda} \int_{U(d)} (U\rho U^{\dagger})^{\otimes n} dU\right\} \tag{127}$$

$$= \sum_{i,j} c_{ij} \text{tr} \left\{ Y_{ij} \int_{U(d)} (U \rho U^\dagger)^{\otimes n} \right\} dU \tag{128}$$

$$= \sum_i c_{ii} \int_{U(d)} \text{tr} \{ Y_{ii} (U \rho U^\dagger)^{\otimes n} \} dU \tag{129}$$

$$= \sum_i c_{ii} \int_{U(d)} \text{tr} \{ U^{\dagger \otimes n} Y_{ii} U^{\otimes n} \rho^{\otimes n} \} dU \tag{130}$$

$$\geq c_{ii} m_{\lambda,n}^{-1} \text{tr} \{ P_\lambda \rho^{\otimes n} \} \tag{131}$$

$$\geq c_{ii} m_{\lambda,n}^{-1} \text{tr} \{ P_{\lambda,\lambda} \rho^{\otimes n} \} \tag{132}$$

$$\geq c_{ii} m_{\lambda,n}^{-1} \frac{\dim(F_\lambda)}{|T_\lambda|} t^{\otimes n}(T_\lambda). \tag{133}$$

We now need to estimate the term $\frac{\dim(F_\lambda)}{|T_\lambda|}$. With $h(i, j)$ denoting the hook-lengths, the dimensions of the irreducible subspaces of any representation of S_n on $(\mathbb{C}^d)^{\otimes n}$ ($d > 0$) obey the following estimates

$$\frac{n!}{\prod_{i=1}^n (\lambda_i + d + 1)!} \leq \frac{n!}{\prod_{(i,j) \in \lambda} h(i, j)} = \dim F_\lambda \leq \frac{n!}{\prod_{i=1}^d \lambda_i!} \quad (\lambda \in \mathbb{Y}_{d,n}). \tag{134}$$

This implies that

$$\frac{\dim(F_\lambda)}{|T_\lambda|} \geq \prod_{i=1}^d \frac{\lambda_i!}{(\lambda_i + d + 1)!} \geq \prod_{i=1}^d \frac{1}{(n + d + 1)^d} = (n + d + 1)^{-d}. \tag{135}$$

Thus,

$$\varepsilon \geq c_{ii} m_{\lambda,n}^{-1} (n + d + 1)^{-d} t^{\otimes n}(T_\lambda) \geq c_{ii} m_{\lambda,n}^{-1} (n + d + 1)^{-d} (2n)^{-d}, \tag{136}$$

leading to $c_{ii} \leq (2dn)^{3d^2} \varepsilon$ for all $i \in [m_{\lambda,n}]$. Now take any vector $x = \sum_i x_i \in V_\lambda$ such that each $x_i \in V_i$, and $\langle x, x \rangle = 1$. Then

$$\langle x, A_\lambda x \rangle = \sum_{i,j} c_{ij} \langle x, Y_{ij} x \rangle \tag{137}$$

$$= \sum_{i,j} c_{ij} \langle x_i, Y_{ij} x_j \rangle \tag{138}$$

$$\leq \sum |c_{ij}| \tag{139}$$

$$\leq \sum_{i,j} \sqrt{|c_{ii}| \cdot |c_{jj}|} \tag{140}$$

$$\leq m_{n,\lambda} (2dn)^{3d^2} \varepsilon \tag{141}$$

$$\leq (2dn)^{4d^2} \varepsilon, \tag{142}$$

and this proves that

$$A_\lambda \leq (2dn)^{4d^2} \varepsilon P_\lambda \quad \forall \lambda \in \mathbb{Y}_{d,n} \tag{143}$$

so that we finally get the desired

$$A \leq (1 - \varepsilon \cdot (2dn)^{4d^2}) \mathbb{1}. \tag{144}$$

□

6. Example

As an example, we consider $d = 2$. Here, the set of states can be identified with the unit ball in \mathbb{R}^3 , and this is also the only reason why we restrict ourselves to that case. Any density operator can be written in the Bloch sphere representation as $\xi = \frac{1}{2}(\mathbb{1} + \sum_{i=1}^3 x_i \sigma_i)$, where $\sigma_1, \sigma_2, \sigma_3 \in \mathcal{B}(\mathbb{C}^2)$ are the usual Pauli matrices, $x_1, x_2, x_3 \in \mathbb{R}$ and $\rho \in \mathcal{S}(\mathbb{C}^2)$ is equivalent to $\sum_{i=1}^3 x_i^2 \leq 1$.

Let $\sigma = \frac{1}{2}(\mathbb{1} + \frac{1}{2}\sigma_3)$, and $\mathfrak{S} = \{\rho : x_3 \leq 1/4\}$. Let us assume that, by using (for some large number n and some small $\varepsilon > 0$), the POVM $\mathcal{M} := \{\mathbb{1} - P_n\} \cup \{P_{f,\lambda}\}_{(f,\lambda) \in \Lambda_\varepsilon}$. The measurement outcome associated to $\mathbb{1} - P_n$ shall be denoted e . But then for every $\rho_s \in \mathfrak{S}$,

$$\text{tr}\{P_{n,s}\rho_s^{\otimes n}\} \geq 1 - (2n)^8 2^{-n \ln(2)\varepsilon^2}. \tag{145}$$

This implies the following. Assume that a state $\xi \in \mathfrak{S} \cup \{\sigma\}$ is being sent, and that we try to find out which state it was. Let \tilde{r}_ρ denote the distribution corresponding to the eigenvalues of the pinching of ρ to the eigenbasis of σ and r_ρ the spectrum of ρ . Define the sets

$$B(f, \lambda) := \{\rho \in \mathfrak{S} \cup \{\sigma\} : \|\tilde{f} - \tilde{r}_\rho\| \leq \varepsilon \bigwedge \|\bar{\lambda} - r_\rho\| \leq \varepsilon\}. \tag{146}$$

After application of our measurement \mathcal{M} to the system, we know the following:

$$\mathbb{P}(\xi = \sigma | \mathcal{M} = e) \geq 1 - 2^{-n \min_{\rho \in \mathfrak{S}} D(\sigma || \rho) - \Theta(n, \varepsilon)} \tag{147}$$

$$\mathbb{P}(\xi \in B(f, \lambda) | \mathcal{M} = (f, \lambda)) \geq 1 - (2n)^8 2^{-n \ln(2)\varepsilon^2}. \tag{148}$$

So, in the end, we can (asymptotically, with high probability) not only distinguish σ from \mathfrak{S} , but to some extent also the elements of \mathfrak{S} from one another (with accuracy ε , and a drawback being that states with the same spectrum and the same pinching to the eigenbasis of σ cannot be distinguished). In our example for $d = 2$, this means that we get the z -coordinate of the true state, and its spectrum (equal to its distance from the origin).

Conclusion

It is an open question whether an even finer decomposition of V_f into a more subtle choice of irreducible subspaces may reveal even more information about the states being measured. A look at pure permutation invariant von Neumann POVMs on the symmetric subspace suggests that there will always be a small ambiguity left.

However, switching to non-optimal (in the sense of Stein’s lemma) measurements that are not permutation-invariant any more (e.g. by concatenating the measurements that are known to be optimal for state discrimination in the sense of Stein’s lemma) might lead to sub-optimal, but information complete, measurements.

The proof of theorem 5 suggests that the ‘quantum method of types’ still needs more refinement: for each $V_{f,\lambda}$, the multiplicity of F_λ in V_f can be larger than one if $d > 2$. This suggests that there is still some information contained in the systems we consider that is not exploited by our approach.

This is in no contradiction to what we said earlier in our example.

More general and asymptotically tight estimates concerning the functions $\rho \mapsto \text{tr}\{P_{f,\lambda}\rho^{\otimes n}\}$ will be dealt with in the second part of this work.

Acknowledgments

This work was supported by the BMBF via grant 01BQ1050, and the hospitality of the Isaac Newton Institute for Mathematical Sciences in the final stages of preparation of this

manuscript is gratefully acknowledged. Many thanks go to Koenraad Audenaert, Fernando Brandao, Matthias Christandl, David Gross, Piotr Śniady and Michael Walter for stimulating discussions.

References

- [1] Ahlswede R 1986 Arbitrarily varying channels with states sequence known to the sender *IEEE Trans. Inform. Theory* **32** 621–9
- [2] Alicki R, Sadowski S and Rudnicki S 1988 Symmetry properties of product states for the system of N n -level atoms *J. Math. Phys.* **29** 1158–62
- [3] Audenaert K M R, Nussbaum M, Szkola A and Verstraete F 2008 Asymptotic error rates in quantum hypothesis testing *Commun. Math. Phys.* **279** 251–83
- [4] Bacon D, Chuang I L and Harrow A W 2007 The quantum Schur and Clebsch–Gordan transforms: I. Efficient qudit circuits *Proc. SODA '07, 18th Annu. ACM-SIAM Symp. on Discrete Algorithms* pp 1235–44
- [5] Bhatia R 1982 Analysis of spectral variation and some inequalities *Trans. Am. Math. Soc.* **272** 323–31
- [6] Bjelaković I, Boche H and Nötzel J 2008 Quantum capacity of a class of compound channels *Phys. Rev. A* **78** 042331
- [7] Bjelaković I and Siegmund-Schultze R 2004 An ergodic theorem for the quantum relative entropy *Commun. Math. Phys.* **247** 697–712
- [8] Bjelaković I, Deuschel J D, Krüger T, Seiler R, Siegmund-Schultze R and Szkola A 2005 A quantum version of Sanov’s theorem *Commun. Math. Phys.* **260** 659–71
- [9] Bjelaković I, Deuschel J D, Krüger T, Seiler R, Siegmund-Schultze R and Szkola A 2008 Typical support and Sanov large deviations of correlated states *Commun. Math. Phys.* **279** 559–84
- [10] Brandão F G S L, Harrow A W, Lee J R and Peres Y 2013 Adversarial hypothesis testing and quantum Stein’s lemma for restricted measurements arXiv:1308.6702
- [11] Brandão F G S L and Plenio M B 2010 A generalization of quantum Stein’s lemma *Commun. Math. Phys.* **295** 791–828
- [12] Christandl M 2006 The structure of bipartite quantum states - insights from group theory and cryptography *PhD Thesis* University of Cambridge
- [13] Christandl M and Mitchison G 2006 The spectra of density operators and the Kronecker coefficients of the symmetric group *Commun. Math. Phys.* **261** 789–97
- [14] Christandl M, Harrow A and Mitchison G 2007 Nonzero Kronecker coefficients and what they tell us about spectra *Commun. Math. Phys.* **270** 575–85
- [15] Christandl M 2008 A quantum information-theoretic proof of the relation between Horn’s problem and the Littlewood–Richardson coefficients *Proc. CiE 2008 (Lecture Notes in Computer Science vol 5028)* pp 120–8
- [16] Christandl M, Sahinoglu M B and Walter M 2012 Recoupling coefficients and quantum entropies arXiv:1210.0463
- [17] Walter M, Doran B, Gross D and Christandl M 2013 Entanglement polytopes *Science* **340** 1205–8
- [18] Csiszár I 1998 The method of types *IEEE Trans. Inf. Theory* **44** 2505–23
- [19] Csiszár I and Körner J 1981 *Information Theory: Coding Theorems for Discrete Memoryless Systems* (New York: Academic)
- [20] Fangwei F and Shiyi S 1996 Hypothesis testing for arbitrarily varying source *Acta Math. Sin.* **12** 33–39
- [21] Fulton W 1997 *Young Tableaux with Applications to Representation Theory and Geometry* (Cambridge: Cambridge University Press)
- [22] Harrow A 2005 Applications of coherent classical communication and the Schur transform to quantum information theory *PhD Thesis* Massachusetts Institute of Technology, Cambridge MA (arXiv:quant-ph/0512255v1)
- [23] Hayashi M 2001 Asymptotics of quantum relative entropy from a representation theoretical viewpoint *J. Phys. A: Math. Gen.* **34** 3413–9
- [24] Hayashi M 2002 Optimal sequence of quantum measurements in the sense of Stein’s lemma in quantum hypothesis testing *J. Phys. A: Math. Gen.* **35** 10759–73
- [25] Hayashi M and Matsumoto K 2002 Quantum universal variable-length source coding *Phys. Rev. A* **66** 022311

- [26] Hiai F, Mosonyi M and Ogawa T 2008 Error exponents in hypothesis testing for correlated states on a spin chain *J. Math. Phys.* **49** 032112
- [27] Hiai F and Petz D 1991 The proper formula for relative entropy and its asymptotics in quantum probability *Commun. Math. Phys.* **143** 99–114
- [28] Horn A 1954 Doubly stochastic matrices and the diagonal of a rotation matrix *Am. J. Math.* **76** 620–30
- [29] Keyl M and Werner R F 2001 Estimating the spectrum of a density operator *Phys. Rev. A* **64** 052311
- [30] Keyl M 2006 Quantum state estimation and large deviations *Rev. Math. Phys.* **18** 19–60
- [31] Milman V D and Schechtman G 2001 *Asymptotic Theory of Finite Dimensional Normed Spaces (Lecture Notes in Mathematics vol 1200)* (Berlin: Springer) (corrected second printing)
- [32] Nötzel J 2012 A solution to two party typicality using representation theory of the symmetric group arXiv:1209.5094
- [33] Ogawa T and Nagaoka H 2000 Strong converse and Stein’s lemma in quantum hypothesis testing *IEEE Trans. Inform. Theory* **46** 2428–33
- [34] Nagaoka H 2001 Strong converse theorems in quantum information theory *Proc. Symp. ‘ERATO Workshop on Quantum Information Science’* p 33
- [35] Schilling C, Gross D and Christandl M 2013 Pinning of fermionic occupation numbers *Phys. Rev. Lett.* **110** 040404
- [36] Sternberg S 1994 *Group Theory and Physics* (Cambridge: Cambridge University Press)
- [37] Thoma E 1964 Die unzerlegbaren, positiv-definiten Klassenfunktionen der abzählbar unendlichen, symmetrischen Gruppe *Math. Z.* **85** 40–61
- [38] Webster R 1994 *Convexity* (Oxford: Oxford University Press)