A de Finetti Representation for Finite Symmetric Quantum States[*]

Robert König and Renato Renner

Computer Science Department
ETH Zürich; Switzerland
rkoenig@inf.ethz.ch   renner@inf.ethz.ch

Abstract

Consider a *symmetric* quantum state on an n-fold product space, that is, the state is invariant under permutations of the n subsystems. We show that, conditioned on the outcomes of an informationally complete measurement applied to a number of subsystems, the state in the remaining subsystems is close to having product form. This immediately generalizes the so-called de Finetti representation to the case of finite symmetric quantum states.

1 Introduction

The analysis of physical experiments is often based on the assumption that the same experiment can be repeated many times independently. In particular, one usually assumes that the results $Z_1, \ldots, Z_n$ obtained from n repetitions of the same experiment are distributed according to some product distribution, i.e., $P_{Z_1 \cdots Z_n} = (P_Z)^n$. In practical situations, however, the independence of the individual outcomes Z_i can usually not be guaranteed.

The so-called de Finetti representation theorem [dF37] can be seen as a solution to this problem[1]. Basically, it states that the assumption on the product structure of $P_{Z_1 \cdots Z_n}$ can be replaced by a seemingly weaker assumption, namely that the distribution of the outcomes of infinitely many repetitions of the experiment are invariant under reordering. For instance, this is the case if the n samples $Z_1, \ldots, Z_n$ are randomly chosen from infinitely many repetitions of the experiment.

Let us briefly explain this result on a more formal level. We say that an n-partite probability distribution $P_{Z_1 \cdots Z_n}$ is *symmetric* if it is invariant under any permutation of the random variables $Z_1, \ldots, Z_n$. If $P_{Z_1 \cdots Z_n}$ is the marginal of a symmetric distribution $P_{Z_1 \cdots Z_m}$ over $m \geq n$ random variables, then $P_{Z_1 \cdots Z_n}$ is called *m-exchangeable*. Moreover, $P_{Z_1 \cdots Z_n}$ is *infinitely exchangeable* if it is m-exchangeable for all $m \geq n$. The result of de Finetti now states that any infinitely exchangeable probability distribution $P_{Z_1 \cdots Z_n}$ can be written as a convex combination of product distributions of the form $(P_Z)^n$.

This result has been generalized in different directions. Diaconis and Freedman [DF80] analyzed the structure of m-exchangeable probability distributions of n random variables, for $n \leq m < \infty$. This is of particular interest for practical applications, where the number of experiments is only finite. They found that, for appropriate values of n and m, these distributions are still close to the convex hull of the set of product distributions.

The result of de Finetti has also been extended to quantum states, to which the notion of symmetry and exchangeability can be adapted in an obvious way. Hudson and Moody [HM76]

---

[1]See [MC93] for a collection of de Finetti's original papers.

showed that any infinitely exchangeable quantum state $\rho^{\overline{n}}$ over n subsystems is a convex combination of product states, i.e., $\rho^{\overline{n}} = \sum_{\mathbf{z}} p_{\mathbf{z}} (\rho_{\mathbf{z}})^{\otimes n}$, for appropriate weights $p_{\mathbf{z}}$ (see also [Hud81]). An alternative proof of this claim has recently been presented by Caves, Fuchs, and Schack [CFS02] (see also [FS04]), relying on the original result of de Finetti.

In this paper, we analyze the structure of m-exchangeable quantum states over n subsystems, for $n \leq m < \infty$. In a sense, our result combines the two mentioned directions of generalizing de Finetti's result. Note that any m-exchangeable state $\rho^{\overline{n}}$ over n subsystems can be extended to an m-exchangeable state $\rho^{\overline{n+k}}$ over $n + k$ subsystems, for $n + k \leq m$. We show that the state $\rho_{\mathbf{z}}^{\overline{n}}$ of the first n subsystems, conditioned on the outcomes $\mathbf{z} = (z_1, \ldots, z_k)$ of an informationally complete measurement applied to each of the remaining k subsystems, is close to a product state $(\rho_{\mathbf{z}})^{\otimes n}$. In particular, since $\rho^{\overline{n}}$ can be written as a convex combination of the states $\rho_{\mathbf{z}}^{\overline{n}}$, i.e., $\rho^{\overline{n}} = \sum_{\mathbf{z}} p_{\mathbf{z}} \rho_{\mathbf{z}}^{\overline{n}}$, this immediately implies that $\rho^{\overline{n}}$ is close to the convex combination $\sum_{\mathbf{z}} p_{\mathbf{z}} (\rho_{\mathbf{z}})^{\otimes n}$. As in the classical case, the distance between the m-exchangeable state $\rho^{\overline{n}}$ and the convex hull of the set of product states depends on the values m and n. In particular, if m is much larger than n, we obtain the result of [HM76] and [CFS02].

Our result has applications in quantum information theory and, in particular, quantum cryptography, e.g., for proving the security of quantum key distribution (QKD) schemes (e.g., [BB84]). An elegant way to study QKD protocols is to subdivide their analysis into two conceptually different stages [Eke91]. In the first stage, Alice and Bob use a quantum channel to distribute n pairs of entangled particles.[2] In the second stage, Alice and Bob each measure their particles and then use the resulting classical information to generate their keys.

For proving the security of such a QKD scheme, one has to show that, even if an adversary can manipulate the state ρ^{AB} of the n particle pairs arbitrarily, either the key generated by Alice and Bob is secure, or they recognize that something went wrong and abort the protocol. However, as the state ρ^{AB} can be arbitrary, these proofs are rather complicated and mostly restricted to a special type of protocol (see also the discussion in [CRE04]). In this context, our results allow to reduce the analysis of ρ^{AB} to the analysis of states which are close to having product form.[3] Such product states correspond to the much simpler situation where the adversary is restricted to attacking each particle individually.

Outline of the paper

In Section 2, we introduce some basic notation and definitions, including the notion of symmetry and exchangeability. Additionally, we briefly review the properties of the variational distance between probability distributions, as well as its quantum analogue, the trace distance between density operators. Sections 3–6 are devoted to the proof of our main results on the structure of symmetric quantum states. Generally speaking, our proof is based on the analysis of the statistics obtained when applying informationally complete POVMs to symmetric quantum states. We will thus be interested in good POVMs in the sense that the measurement statistics gives maximal information about the measured state. Constructing such POVMs is the main purpose of Section 3, which is somehow independent of the remaining part of the paper. In Section 4, we analyze classical symmetric probability distributions and derive bounds on their distance to product distributions. In Section 5, it is shown how to deduce structural properties of quantum states from the corresponding properties of the measurement statistics, using the POVMs constructed in Section 3. Finally, in Section 6, we combine these results to obtain our main statements, including a de Finetti representation for finitely exchangeable quantum states.

---

[2]In many practical QKD protocols, Alice prepares particles according to some classical randomness and then uses the quantum channel to send them to Bob. However, for analyzing such a protocol, one can equivalently think of a protocol where Alice prepares pairs of fully entangled particles and then sends one particle of each pair to Bob while keeping the other one.

[3]More precisely, conditioned on the outcome of certain statistical tests performed during the protocol (e.g., for estimating the error rate), the state of any small subset of particle pairs randomly chosen by Alice and Bob is close to a product state.

Additionally, in Appendix A, we present an alternative version of our results which might be more suitable for certain applications.

2 Preliminaries

2.1 Density operators, POVMs, and probability distributions

Throughout this paper, we will restrict our attention to finite-dimensional Hilbert spaces, denoted by $\mathcal{H}$ or $\mathcal{H}_A$, for some index A. Let $\mathrm{End}(\mathcal{H})$ be the set of endomorphisms on $\mathcal{H}$, and $\mathrm{Herm}(\mathcal{H})$ the set of hermitian endomorphisms on $\mathcal{H}$. An element $\rho \in \mathrm{Herm}(\mathcal{H})$ is called a *density operator* or, equivalently, a *quantum state* on $\mathcal{H}$ if it is positive semidefinite, $\rho \geq 0$, and has trace one, $\mathrm{tr}(\rho) = 1$. We denote by $\mathrm{S}(\mathcal{H})$ the set of density operators on $\mathcal{H}$. A *positive operator valued measure (POVM)* on $\mathcal{H}$ is a family $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ of nonnegative operators $F_z \in \mathrm{Herm}(\mathcal{H})$, $F_z \geq 0$, such that $\sum_{z \in \mathcal{Z}} F_z = \mathrm{id}_{\mathcal{H}}$. The POVM $\mathfrak{Z}$ is called *informationally complete* if it is a basis of $\mathrm{Herm}(\mathcal{H})$.

To improve the readability of formulas involving density operators on product spaces, we use superscripts to indicate which subsystems an operator acts on, e.g., we write ρ^{ABC} for a density operator on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Operators with the same name but different superscripts are related to each other by the partial trace. For example, ρ^{AB} is the partial state obtained from ρ^{ABC} by tracing over $\mathcal{H}_C$, i.e., $\rho^{AB} = \mathrm{Tr}_C(\rho^{ABC})$, and, similarly, $\rho^A = \mathrm{Tr}_{BC}(\rho^{ABC})$. This notation is consistent since partial traces over different subsystems commute, e.g., we have $\rho^A = \mathrm{Tr}_B(\rho^{AB}) = \mathrm{Tr}_C(\rho^{AC}) = \mathrm{Tr}_{BC}(\rho^{ABC})$.

A similar formalism can be used to denote conditional quantum states. Let ρ^{AB} be a density operator on $\mathcal{H}_A \otimes \mathcal{H}_B$ and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}_B$. Then $\rho^A{}_{|\mathfrak{Z}=z}$ denotes the quantum state on $\mathcal{H}_A$ conditioned on the event that the outcome of the measurement $\mathfrak{Z}$ applied to the subsystem $\mathcal{H}_B$ equals $z \in \mathcal{Z}$, i.e.,

$$\rho^A{}_{|\mathfrak{Z}=z} := \frac{1}{\mathrm{tr}((\mathrm{id}_A \otimes F_z)\rho^{AB})} \mathrm{Tr}_B\big((\mathrm{id}_A \otimes F_z)\rho^{AB}\big) \ .$$

The notation can be extended to density operators over three and more subsystems in an obvious way. Note that, since the partial trace and the operation of conditioning on a measurement result commute, this is compatible with our notation for partial states. For instance, if ρ^{ABC} is a tripartite density operator, then the conditional states $\rho^A{}_{|\mathfrak{Z}=z}$ and $\rho^{AC}{}_{|\mathfrak{Z}=z}$ are related by the partial trace, i.e., $\rho^A{}_{|\mathfrak{Z}=z} = \mathrm{Tr}_C(\rho^{AC}{}_{|\mathfrak{Z}=z})$.

We will use a similar formalism to denote the probability distributions resulting from measurements of quantum states. Let ρ^A be a density operator and let $\mathfrak{Y} = \{E_y\}_{y \in \mathcal{Y}}$ be a POVM on $\mathcal{H}_A$. Then $\rho^A_{\mathfrak{Y}}$ denotes the distribution of the outcome of the measurement $\mathfrak{Y}$ applied to ρ^A, i.e.,

$$\rho^A_{\mathfrak{Y}}(z) = \mathrm{tr}(E_y \rho) \ , \qquad \text{for all } y \in \mathcal{Y}.$$

This can easily be generalized to product systems. For example, if $\mathfrak{Y}$ and $\mathfrak{Z}$ are POVMs on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then $\rho^{AB}_{\mathfrak{Y}\mathfrak{Z}}$ is the probability distribution of the outcome of the product measurement $\mathfrak{Y} \otimes \mathfrak{Z}$ applied to ρ^{AB}.

Note that the operation of taking the partial trace of a density operator has a classical analogue, namely taking the marginal distribution. Similarly, the operation of conditioning a quantum state on a measurement result corresponds to conditioning a probability distribution on the value of a random variable. Our formalism is consistent with respect to these operations in the sense that the following diagram commutes.

$$
\begin{array}{ccccc}
\rho^A{}_{|\mathfrak{Z}=z} & \xleftarrow{\ \text{cond.}\ } & \rho^{AB} & \xrightarrow{\ \text{trace}\ } & \rho^A \\
{\scriptstyle\text{meas.}}\big\downarrow & & {\scriptstyle\text{meas.}}\big\downarrow & & {\scriptstyle\text{meas.}}\big\downarrow \\
\rho^A_{\mathfrak{Y}|\mathfrak{Z}=z} & \xleftarrow{\ \text{cond.}\ } & \rho^{AB}_{\mathfrak{Y}\mathfrak{Z}} & \xrightarrow{\ \text{trace}\ } & \rho^A_{\mathfrak{Y}}
\end{array}
$$

3

Let P be a probability distribution on $\mathcal{Z}$ and let, for each $z \in \mathcal{Z}$, ρ_z be a density operator on $\mathcal{H}$. We will often write the weighted sum of ρ_z as an expectation value, i.e.,

$$\mathbb{E}_{z \leftarrow P}[\rho_z] := \sum_{z \in \mathcal{Z}} P(z)\rho_z \ .$$

If the probability distribution is clear from the context, we only write $\mathbb{E}_z[\rho_z]$. For example, using our formalism, we have

$$\mathbb{E}_{z \leftarrow \rho_3^B}[\rho^A|_{3=z}] = \rho^A \ , \tag{1}$$

for any bipartite quantum state ρ^{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$. This is a simple reformulation of the fact that the partial state ρ^A on $\mathcal{H}_A$ does not change when a measurement is applied to the subsystem $\mathcal{H}_B$.

2.2   Distance measures

Let $\mathrm{Distr}(\mathcal{Z})$ be the set of probability distributions on the set $\mathcal{Z}$. The *variational distance* between two probability distributions $P, Q \in \mathrm{Distr}(\mathcal{Z})$ is defined by

$$\delta(P, Q) := \frac{1}{2} \sum_{z \in \mathcal{Z}} |P(z) - Q(z)| \ .$$

The variational distance is a metric on $\mathrm{Distr}(\mathcal{Z})$. In particular, $\delta(P, Q) = 0$ if and only if $P = Q$, δ is symmetric, $\delta(P, Q) = \delta(Q, P)$, and the triangle inequality holds, $\delta(P, R) \leq \delta(P, Q) + \delta(Q, R)$. For two bipartite distributions P_{XY} and $P_{X'Y'}$, the variational distance cannot increase when taking the marginals,

$$\delta(P_X, P_{X'}) \leq \delta(P_{XY}, P_{X'Y'}) \ . \tag{2}$$

If P_{XY} and $P_{X'Y'}$ have the same marginals $P_X = P_{X'}$, their distance can be expressed as the expectation value of the distance between their conditional probability distributions,

$$\delta(P_{XY}, P_{X'Y'}) = \mathbb{E}_{x \leftarrow P_X}\big[\delta(P_{Y|X=x}, P_{Y'|X'=x})\big] := \sum_x P_X(x)\, \delta(P_{Y|X=x}, P_{Y'|X'=x}) \ . \tag{3}$$

In particular, if the distributions have product form,

$$\delta(P_X \times P_Y, P_X \times P_{Y'}) = \delta(P_Y, P_{Y'}) \ . \tag{4}$$

A similar distance measure can be defined on the set $\mathrm{Herm}(\mathcal{H})$ of hermitian operators on $\mathcal{H}$. The *trace distance* between two operators $U, V \in \mathrm{Herm}(\mathcal{H})$ is defined by

$$\delta(U, V) := \frac{1}{2}\mathrm{tr}|U - V| \ .$$

Many properties of the variational distance also hold for the trace distance. In particular, the trace distance is a metric on $\mathrm{Herm}(\mathcal{H})$. Moreover, similarly to (2), the trace distance cannot increase when taking the partial trace, i.e., for $U, V \in \mathrm{Herm}(\mathcal{H}_A \otimes \mathcal{H}_B)$,

$$\delta\big(\mathrm{Tr}_B(U), \mathrm{Tr}_B(V)\big) \leq \delta(U, V) \ . \tag{5}$$

We will also use the strong convexity of the trace distance, i.e., for $U, U', V, V' \in \mathrm{Herm}(\mathcal{H})$ and $p, q \in [0, 1]$ with $p + q = 1$,

$$\delta(pU + qU', pV + qV') \leq p\, \delta(U, V) + q\, \delta(U', V') \ .$$

The following lemma gives a simple expression for the trace distance between two product operators $U \otimes V$ and $U' \otimes V$ with a common factor V.

4

Lemma 2.1. *Let $U, U' \in \operatorname{Herm}(\mathcal{H}_A)$ and $V \in \operatorname{Herm}(\mathcal{H}_B)$. Then*

$$\delta(U \otimes V, U' \otimes V) = \delta(U, U') \cdot \operatorname{tr}(|V|).$$

Proof. By definition,

$$\delta(U \otimes V, U' \otimes V) = \operatorname{tr}|(U - U') \otimes V|. \tag{6}$$

We use the following general fact, which can be verified easily using the appropriate definitions. Let $f : \mathbb{C} \to \mathbb{C}$ a function satisfying

$$f(a \cdot b) = f(a) \cdot f(b) \qquad \text{for all } a, b \in \mathbb{C}.$$

Then

$$f(A \otimes B) = f(A) \otimes f(B)$$

for all $A, B \in \operatorname{Herm}(\mathcal{H})$. Applying this to equation (6) yields

$$|(U - U') \otimes V| = |(U - U')| \otimes |V| \ .$$

The assertion then follows from the identity $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \cdot \operatorname{tr}(B)$. $\qquad\square$

As an immediate consequence of Lemma 2.1, we obtain the equation

$$\delta(\rho \otimes \sigma, \rho' \otimes \sigma) = \delta(\rho, \rho') \ , \tag{7}$$

for states $\rho, \rho' \in S(\mathcal{H}_A)$ and $\sigma \in S(\mathcal{H}_B)$, which is the quantum analogue of (4). The trace distance between two density operators ρ and σ on $\mathcal{H}$ corresponds to the variational distance between the probability distributions $\rho_{\mathfrak{Z}}$ and $\sigma_{\mathfrak{Z}}$ of the outcomes of a measurement applied to ρ and σ, respectively, for an optimal POVM $\mathfrak{Z}$ on $\mathcal{H}$, i.e.,

$$\delta(\rho, \sigma) = \max_{\mathfrak{Z}} \delta(\rho_{\mathfrak{Z}}, \sigma_{\mathfrak{Z}}) \ . \tag{8}$$

2.3 Symmetry and exchangeability

2.3.1 Symmetric probability distributions and symmetric functions

Let $\mathbf{z} = (z_1, \ldots, z_n) \in \mathcal{Z}^n$ and $\mathbf{z}' = (z'_1, \ldots, z'_m) \in \mathcal{Z}^m$ be tuples of elements from a set $\mathcal{Z}$. We denote by $(\mathbf{z}, \mathbf{z}')$ the $(n + m)$-tuple obtained by concatenating $\mathbf{z}$ and $\mathbf{z}'$, $(\mathbf{z}, \mathbf{z}') := (z_1, \ldots, z_n, z'_1, \ldots, z'_m)$.

The *frequency distribution* $Q_{\mathbf{z}}$ of an n-tuple $\mathbf{z} = (z_1, \ldots, z_n) \in \mathcal{Z}^n$ is the function on $\mathcal{Z}$ defined by[4]

$$Q_{\mathbf{z}}(z) := \frac{1}{n} \big| \{ i \in [n] : z_i = z \} \big| \ , \quad \text{for every } z \in \mathcal{Z},$$

i.e., $Q_{\mathbf{z}}(z)$ is the relative number of occurrences of the symbol z in $\mathbf{z}$. Note that $Q_{\mathbf{z}}$ is a probability distribution on $\mathcal{Z}$, $Q_{\mathbf{z}} \in \operatorname{Distr}(\mathcal{Z})$.

A symmetric function f on $\mathcal{Z}^n$ is a function such that $f(\mathbf{z})$ is invariant under permutations of the entries in $\mathbf{z}$. In particular, the value $f(\mathbf{z})$ only depends on the frequency distribution $Q_{\mathbf{z}}$ of $\mathbf{z}$. For a formal definition, let S_n be the set of permutations on $[n]$, and let, for any $\pi \in S_n$, $\pi_{\mathcal{Z}}$ be the bijection on $\mathcal{Z}^n$ defined by

$$\pi_{\mathcal{Z}} : (z_1, \ldots, z_n) \longmapsto (z_{\pi(1)}, \ldots, z_{\pi(n)}) \ , \qquad \text{for all } (z_1, \ldots, z_n) \in \mathcal{Z}^n.$$

Definition 2.2. *A function f with domain $\mathcal{Z}^n$ is called* symmetric *if*

$$f = f \circ \pi_{\mathcal{Z}} \ , \qquad \text{for all } \pi \in S_n.$$

---

[4] We denote by $[n]$ the set of natural numbers between 1 and n, i.e., $[n] := \{1, \ldots, n\}$.

In particular, a probability distribution $P_{\mathbf{Z}} \in \text{Distr}(\mathcal{Z}^n)$ on $\mathcal{Z}^n$ is called *symmetric* if $P_{\mathbf{Z}}$ is a symmetric function. The following lemma is an immediate consequence of these definitions.

Lemma 2.3. *Let $\mathbf{Z}$ be an n-tuple of random variables over a set $\mathcal{Z}$ such that $P_{\mathbf{Z}}$ is symmetric, and let Y be a random variable over $\mathcal{Y}$ defined by a channel $P_{Y|\mathbf{Z}}$ such that for every $y \in \mathcal{Y}$, the function $\mathbf{z} \mapsto P_{Y|\mathbf{Z}=\mathbf{z}}(y)$ is symmetric. Then, for every $y \in \mathcal{Y}$, the conditional probability distribution $P_{\mathbf{Z}|Y=y}$ is symmetric.*

In particular, if $f : \mathcal{Z}^n \to \mathcal{Y}$ is a symmetric function, then, for any $y \in \mathcal{Y}$, $P_{\mathbf{Z}|f(\mathbf{Z})=y}$ is symmetric. An example is the function mapping any n-tuple $\mathbf{z}$ to the frequency distribution $Q_{\mathbf{z}}$, i.e., $P_{\mathbf{Z}|Q_{\mathbf{z}}=q}$ is symmetric.[5] The following lemma is an immediate consequence of this fact.

Lemma 2.4. *Let $\mathbf{Z} = (Z_1, \ldots, Z_n)$ be an n-tuple of random variables over a set $\mathcal{Z}$ such that $P_{\mathbf{Z}}$ is symmetric. Then, for any $q \in \text{Distr}(\mathcal{Z})$,*

$$P_{Z_i|Q_{\mathbf{Z}}=q} = q \ , \quad \text{for every } i \in [n].$$

2.3.2 Symmetric and exchangeable density operators

For any permutation $\pi \in S_n$, let $\pi_{\mathcal{H}}$ be the unique endomorphism on $\mathcal{H}^{\otimes n}$ satisfying

$$\pi_{\mathcal{H}}(|\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle) = |\phi_{\pi(1)}\rangle \otimes \cdots \otimes |\phi_{\pi(n)}\rangle \ , \qquad \text{for all } |\phi_1\rangle, \ldots, |\phi_n\rangle \in \mathcal{H}.$$

It is easy to verify that $\pi_{\mathcal{H}} \in \text{End}(\mathcal{H}^{\otimes n})$ is unitary. A density operator $\rho^{B_1 \cdots B_n} \in \text{End}(\mathcal{H}^{\otimes n})$ is called *symmetric* if $\rho^{B_1 \cdots B_n} = \pi_{\mathcal{H}} \rho^{B_1 \cdots B_n} \pi_{\mathcal{H}}^{\dagger}$ for every $\pi \in S_n$. The following definition generalizes this concept to include an additional system $\mathcal{H}_A$.

Definition 2.5. *A density operator $\rho^{AB_1 \cdots B_n} \in \text{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n})$ is called symmetric relative to $\mathcal{H}_A$ if*

$$\rho^{AB_1 \cdots B_n} = (\text{id}_A \otimes \pi_{\mathcal{H}}) \rho^{AB_1 \cdots B_n} (\text{id}_A \otimes \pi_{\mathcal{H}}^{\dagger}) \ , \qquad \text{for all } \pi \in S_n.$$

Let $\rho^{AB_1 \cdots B_n} \in \text{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n})$ be symmetric relative to $\mathcal{H}_A$. Then, for any choice of r distinct indices $i_1, \ldots, i_r \in [n]$, $r \in [n]$, the state $\rho^{AB_{i_1} \cdots B_{i_r}}$ is symmetric relative to $\mathcal{H}_A$. Moreover, since it only depends on the number r of distinct indices, we will write $\rho^{A\overline{r}}$ instead of $\rho^{AB_{i_1} \cdots B_{i_r}}$.

Similarly, for every $\mathbf{z} \in \mathcal{Z}^s$, the density operator $\rho^{AB_{i_1} \cdots B_{i_{n-s}}}_{|\mathfrak{Z}^{\otimes s}=\mathbf{z}}$ obtained by conditioning a symmetric state $\rho^{A\overline{n}} = \rho^{AB_1 \cdots B_n}$ on the outcomes of a POVM $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ applied to s subsystems is independent of the indices $i_1, \ldots, i_{n-s}$. Additionally, as an immediate consequence of Lemma 2.6 below, this conditional state is still symmetric relative to $\mathcal{H}_A$. We will thus use the abbreviation $\rho^{A\overline{n-s}}_{|\mathfrak{Z}^s=\mathbf{z}}$.

Lemma 2.6. *Let $\rho^{AB\overline{n}} \in \text{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}^{\otimes n})$ be symmetric relative to $\mathcal{H}_A \otimes \mathcal{H}_B$. Then, for any POVM $\mathfrak{Y} = \{E_y\}_{y \in \mathcal{Y}}$ on $\mathcal{H}_A$ and every $y \in \mathcal{Y}$, $\rho^{B\overline{n}}_{|\mathfrak{Y}=y}$ is symmetric relative to $\mathcal{H}_B$.*

Proof. It suffices to show that, for any $\pi \in S_n$ and any $y \in \mathcal{Y}$,

$$(\text{id}_B \otimes \pi_{\mathcal{H}})\text{Tr}_A\big((E_y \otimes \text{id}_{B\overline{n}})\rho^{AB\overline{n}}\big)(\text{id}_B \otimes \pi_{\mathcal{H}}^{\dagger}) = \text{Tr}_A\big((E_y \otimes \text{id}_{B\overline{n}})\rho^{AB\overline{n}}\big)$$

where $\text{id}_{B\overline{n}} := \text{id}_B \otimes \text{id}_{\mathcal{H}}^{\otimes n}$. We use the general identity

$$U\text{Tr}_A(W)U' = \text{Tr}_A\big((\text{id}_A \otimes U)W(\text{id}_A \otimes U')\big)$$

where $U, U' \in \text{End}(\mathcal{H}_B)$ and $W \in \text{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$, setting $U := \text{id}_B \otimes \pi_{\mathcal{H}}$, $U' := \text{id}_B \otimes \pi_{\mathcal{H}}^{\dagger}$, and $W := (E_y \otimes \text{id}_{B\overline{n}})\rho^{AB\overline{n}}$. This leads to

$$
\begin{aligned}
(\text{id}_B \otimes \pi_{\mathcal{H}})\text{Tr}_A&\big((E_y \otimes \text{id}_{B\overline{n}})\rho^{AB\overline{n}}\big)(\text{id}_B \otimes \pi_{\mathcal{H}}^{\dagger}) \\
&= \text{Tr}_A\big((\text{id}_{AB} \otimes \pi_{\mathcal{H}})(E_y \otimes \text{id}_{B\overline{n}})\rho^{AB\overline{n}}(\text{id}_{AB} \otimes \pi_{\mathcal{H}}^{\dagger})\big) \\
&= \text{Tr}_A\big((E_y \otimes \text{id}_{B\overline{n}})(\text{id}_{AB} \otimes \pi_{\mathcal{H}})\rho^{AB\overline{n}}(\text{id}_{AB} \otimes \pi_{\mathcal{H}}^{\dagger})\big)
\end{aligned}
$$

---

[5]$P_{Q_{\mathbf{Z}}}$ denotes the probability distribution of $Q_{\mathbf{z}}$, for $\mathbf{z}$ randomly chosen according to $P_{\mathbf{Z}}$, that is, $P_{Q_{\mathbf{Z}}}(q) := \mathbb{P}_{\mathbf{z} \leftarrow P_{\mathbf{Z}}}[Q_{\mathbf{z}} = q]$.

The assertion then follows since $\rho^{AB\overline{n}}$ is symmetric relative to $\mathcal{H}_A \otimes \mathcal{H}_B$, that is,

$$(\mathrm{id}_{AB} \otimes \pi_\mathcal{H})\rho^{AB\overline{n}}(\mathrm{id}_{AB} \otimes \pi_\mathcal{H}^\dagger) = \rho^{AB\overline{n}} \ . \qquad \square$$

The notation for symmetric quantum states introduced above can also be used to denote symmetric probability distributions, e.g., resulting from measuring a symmetric quantum state. Let, for instance, $\rho^{A\overline{n}} = \rho^{AB_1 \cdots B_n} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n})$ be symmetric relative to $\mathcal{H}_A$. Then, for POVMs $\mathfrak{Y}$ and $\mathfrak{Z}$ on $\mathcal{H}_A$ and $\mathcal{H}$, respectively, we write $\rho^{A\overline{n}}_{\mathfrak{Y}\overline{\mathfrak{Z}}}$ instead of $\rho^{AB_1 \cdots B_n}_{\mathfrak{Y}\,\mathfrak{Z}\,\cdots\,\mathfrak{Z}}$.

To formulate our theorems in a compact way, we will make use of the notion of exchangeability. A symmetric density operator $\rho^{\overline{n}} \in \mathrm{S}(\mathcal{H}^{\otimes n})$ is said to be m-exchangeable, for $m \geq n$, if there exists a symmetric density operator $\sigma^{\overline{m}} \in \mathrm{S}(\mathcal{H}^{\otimes m})$ such that $\rho^{\overline{n}}$ is the partial trace of $\sigma^{\overline{m}}$, i.e., $\rho^{\overline{n}} = \sigma^{\overline{n}}$. Similarly to Definition 2.5, the definition of exchangeability can be generalized to include an additional system $\mathcal{H}_A$.

Definition 2.7. *A density operator $\rho^{A\overline{n}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n})$ which is symmetric relative to $\mathcal{H}_A$ is called m-exchangeable relative to $\mathcal{H}_A$ if there exists a density operator $\sigma^{A\overline{m}} \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes m})$ such that $\sigma^{A\overline{n}}$ is symmetric relative to $\mathcal{H}_A$ and $\rho^{A\overline{n}} = \sigma^{A\overline{n}}$. We refer to $\sigma^{A\overline{m}}$ as an* extension *of $\rho^{A\overline{n}}$.*

In the following, we will often use the same label for an extension of a state. For example, we will denote an extension of $\rho^{A\overline{n}}$ to m systems (for $m \geq n$) by $\rho^{A\overline{m}}$.

2.4 Dual basis and quantum tomography

Definition 2.8. *Let $\{e_i\}_{i \in \mathcal{N}}$ be a family of vectors in a Hilbert space $\mathcal{H}$. A family $\{f_i\}_{i \in \mathcal{N}}$ is called a* dual *of $\{e_i\}_{i \in \mathcal{N}}$ if*

$$v = \sum_{i \in \mathcal{N}} \langle f_i | v \rangle e_i \ , \quad \text{for all } v \in \mathcal{H},$$

where $\langle f_i | v \rangle$ denotes the inner product between f_i and v.

Without proof, we state the following lemma known from linear algebra.

Lemma 2.9. *If $\{f_i\}_{i \in \mathcal{N}}$ is a basis of $\mathcal{H}$, then there exists a unique family $\{e_i\}_{i \in \mathcal{N}}$ such that $\{f_i\}_{i \in \mathcal{N}}$ is a dual of $\{e_i\}_{i \in \mathcal{N}}$.*

Note that the set $\mathrm{End}(\mathcal{H})$ of endomorphisms on $\mathcal{H}$ forms a complex Hilbert space with inner product $(U, V) \mapsto \mathrm{tr}(UV^\dagger)$. Similarly, the set $\mathrm{Herm}(\mathcal{H})$ of hermitian operators on $\mathcal{H}$ is a real Hilbert space with inner product $(U, V) \mapsto \mathrm{tr}(UV)$. Hence, a family $\{F_z\}_{z \in \mathcal{Z}}$ of elements from $\mathrm{Herm}(\mathcal{H})$ is a dual of a family $\{F_z^*\}_{z \in \mathcal{Z}}$ if

$$U = \sum_{z \in \mathcal{Z}} \mathrm{tr}(F_z U) F_z^* \ , \quad \text{for all } U \in \mathrm{Herm}(\mathcal{H}). \tag{9}$$

In particular, expression (9) states that the operator U is fully determined by the values of the traces $\mathrm{tr}(F_z U)$. The following lemma generalizes this fact to product spaces.

Lemma 2.10. *Let $\{F_z\}_{z \in \mathcal{Z}}$ and $\{F_z^*\}_{z \in \mathcal{Z}}$ be families of elements from $\mathrm{Herm}(\mathcal{H}_B)$ such that $\{F_z\}_{z \in \mathcal{Z}}$ is the dual of $\{F_z^*\}_{z \in \mathcal{Z}}$. Then, for any $W \in \mathrm{Herm}(\mathcal{H}_A \otimes \mathcal{H}_B)$,*

$$W = \sum_{z \in \mathcal{Z}} W_z \otimes F_z^* \ ,$$

where $W_z := \mathrm{Tr}_B((\mathrm{id}_A \otimes F_z)W)$, for all $z \in \mathcal{Z}$.

Proof. It is easy to verify that $\mathrm{Herm}(\mathcal{H}_A \otimes \mathcal{H}_B) = \mathrm{Herm}(\mathcal{H}_A) \otimes \mathrm{Herm}(\mathcal{H}_B)$. Hence there exist operators $U_i \in \mathrm{Herm}(\mathcal{H}_A)$ and $V_i \in \mathrm{Herm}(\mathcal{H}_B)$ such that $W = \sum_i U_i \otimes V_i$. By the linearity of the sum and the trace operator, it thus suffices to show that

$$U \otimes V = \sum_{z \in \mathcal{Z}} \mathrm{Tr}_B\big((\mathrm{id}_A \otimes F_z)(U \otimes V)\big) \otimes F_z^*$$

for any $U \in \mathrm{Herm}(\mathcal{H}_A)$ and $V \in \mathrm{Herm}(\mathcal{H}_B)$. Since Tr_B can be written as $\mathrm{Tr}_B = \mathrm{id}_A \otimes \mathrm{tr}_B$ (where $\mathcal{H}_A \otimes \mathbb{C}$ is identified with $\mathcal{H}_A$) we find

$$\mathrm{Tr}_B\big((\mathrm{id}_A \otimes F_z)(U \otimes V)\big) = \mathrm{Tr}_B\big(U \otimes (F_z V)\big) = \mathrm{tr}(F_z V)U \ ,$$

and thus

$$\sum_{z \in \mathcal{Z}} \mathrm{Tr}_B\big((\mathrm{id}_A \otimes F_z)(U \otimes V)\big) \otimes F_z^* = U \otimes \left(\sum_{z \in \mathcal{Z}} \mathrm{tr}(F_z V)F_z^*\right)$$

The assertion then follows from (9). $\qquad\qquad\square$

Let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}_B$ and let $\{F_z^*\}_{z \in \mathcal{Z}}$ be a family of elements from $\mathrm{Herm}(\mathcal{H}_B)$ such that $\{F_z\}_{z \in \mathcal{Z}}$ is the dual of $\{F_z^*\}_{z \in \mathcal{Z}}$. Definition 9 directly implies that any density operator ρ^B on $\mathcal{H}_B$ can be written as

$$\rho^B = \mathop{\mathbb{E}}_{z \leftarrow \rho^B_{\mathfrak{Z}}} \big[F_z^*\big] \ , \tag{10}$$

i.e., ρ^B is fully determined by the probability distribution $\rho^B_{\mathfrak{Z}}$ of the outcomes when applying the measurement $\mathfrak{Z}$ on ρ^B. On the other hand, it is an immediate consequence of Lemma 2.10 that, for any density operator ρ^{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$,

$$\rho^{AB} = \mathop{\mathbb{E}}_{z \leftarrow \rho^B_{\mathfrak{Z}}} \big[\rho^A_{|\mathfrak{Z}=z} \otimes F_z^*\big] \ . \tag{11}$$

The above formulas are useful for quantum state tomography, that is, the reconstruction of an unknown quantum state ρ given only the statistics of measurement applied to identical copies of ρ. For example, it follows from (10), the strong convexity of the trace distance and Lemma 2.1 that the estimate $\tilde{\rho}^B := \mathbb{E}_{z \leftarrow \tilde{P}_Z}\big[F_z^*\big]$ is close to ρ^B,

$$\delta(\rho^B, \tilde{\rho}^B) \leq \sum_{z \in \mathcal{Z}} \big|P_Z(z) - \tilde{P}_Z(z)\big| \cdot \mathrm{tr}|F_z^*| \ . \tag{12}$$

In particular, in order to obtain good estimates, one should choose a POVM $\mathfrak{Z}$ such that the traces $\mathrm{tr}|F_z^*|$ are small.

3 Informationally complete POVMs and duals

3.1 Symmetric informationally complete POVMs

Intuitively, a POVM $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ is useful for tomography if the distance between any two operators F_z and $F_{z'}$ is large. This is for instance the case for symmetric POVMs as defined below, where the operators F_z are symmetrically distributed over the space of positive operators.

Definition 3.1. *Let $\mathcal{H}$ be a d-dimensional Hilbert space. A* symmetric *informationally complete POVM $\mathfrak{Z} = \{F_z\}_{z \in [d^2]}$ on $\mathcal{H}$ is an informationally complete POVM that consists of rank-one projectors*

$$F_z := \frac{1}{d}|\psi_z\rangle\langle\psi_z| \qquad \textit{for all } z \in [d^2]$$

with the property that

$$\mathrm{tr}(F_z F_{z'}) = \theta_d \qquad \textit{for all } z \neq z'.$$

for some $\theta_d \in \mathbb{C}$.

Analytic constructions of symmetric informationally complete POVMs are known for dimensions $d = 2, 3, 4, 6, 8$ (see, e.g., [RBKSC04, Gra04]). It can be shown that if a symmetric informationally complete POVM exists in dimension d, then θ_d is a universal constant which is independent of the particular symmetric informationally complete POVM. It equals

$$\theta_d = \frac{1}{d^2(d+1)}.$$

Lemma 3.2. *Let $\mathfrak{Z} = \{F_z\}_{z \in [d^2]} \in \text{POVM}_{\mathcal{H}}$ be a symmetric informationally complete POVM on a d-dimensional Hilbert space $\mathcal{H}$. Then there is a set of operators $\{F_z^*\}_{z \in [d^2]} \subset \text{Herm}(\mathcal{H})$ that satisfies*

(i). *$\mathfrak{Z}$ is a dual of $\{F_z^*\}_{z \in [d^2]}$.*

(ii). *For every $z \in [d^2]$, the eigenvalues of F_z^* and their multiplicities are*

$$
\begin{aligned}
\lambda_0 &:= d & n_0 &:= 1 \\
\lambda_1 &:= -1 & n_1 &:= d - 1.
\end{aligned}
$$

Proof. Let us define $\alpha := d^2 + d - 1$. It is straightforward to verify that the operators

$$
F_z^* := \alpha F_z - \sum_{z' \neq z} F_{z'} \qquad z \in [d^2]
$$

satisfy $\text{tr}(F_z^* F_{z'}) = \delta_{zz'}$, where $\delta_{zz'}$ denotes the Kronecker-delta, which equals one if $z = z'$ and 0 otherwise. This implies property (i). To obtain their eigenvalues, consider the matrix

$$
B := F_z^* + \text{id} = (\alpha + 1)F_z.
$$

Because $F_z = \frac{1}{d}|\psi_z\rangle\langle\psi_z|$, the eigenvalues of B are $\frac{\alpha+1}{d}$ and 0, occurring with multiplicities 1 and $d - 1$, respectively. Hence statement (ii) follows. $\qquad\square$

3.2 A construction for arbitrary dimensions

As mentioned in the previous section, symmetric informationally complete POVMs are suitable for tomography. However, their existence is only proven for certain dimensions. In this section, we will give a construction of informationally complete POVMs for any dimension. It is motivated by a general group-theoretic technique for finding such POVMs (see e.g., [DPS04]).

Let $\mathcal{H}$ be a d-dimensional Hilbert space and let $\omega := e^{\frac{2\pi i}{d}}$ be the d-th primitive root of unity. Define the operators

$$
D_{jk} := \omega^{\frac{j \odot k}{2}} \sum_{m \in \mathbb{Z}_d} \omega^{jm} |k \oplus m\rangle\langle m| \qquad \text{for all } (j, k) \in \mathbb{Z}_d \times \mathbb{Z}_d,
$$

where $\oplus, \odot$ denotes addition and multiplication modulo d, respectively. Furthermore, define

$$
c((j, k), (l, m)) := jm - kl \qquad \text{for all } (j, k), (l, m) \in \mathbb{Z}_d \times \mathbb{Z}_d.
$$

We will use the simple identity

$$
\sum_{\beta \in \mathbb{Z}_d \times \mathbb{Z}_d} \omega^{c(\alpha, \beta)} = d^2 \cdot \delta_{\alpha, 0} \qquad \text{for all } \alpha \in \mathbb{Z}_d \times \mathbb{Z}_d. \tag{13}
$$

where $\delta_{\alpha, \beta}$ denotes the Kronecker-delta, which equals 1 if $\alpha = \beta$ and 0 otherwise. Note that this identity directly follows from

$$
\sum_{m \in \mathbb{Z}_d} \omega^{km} = d \cdot \delta_{k, 0} \qquad \text{for all } k \in \mathbb{Z}_d. \tag{14}
$$

Lemma 3.3. *The operators $\{D_\alpha\}_{\alpha \in \mathbb{Z}_d \times \mathbb{Z}_d}$ have the following properties.*

(i). *D_α is unitary for every $\alpha \in \mathbb{Z}_d \times \mathbb{Z}_d$.*

(ii). *For every $\rho \in \text{S}(\mathcal{H})$, $\sum_{\alpha \in \mathbb{Z}_d \times \mathbb{Z}_d} D_\alpha \rho D_\alpha^\dagger = d \cdot \text{id}$.*

(iii). *$D_\alpha D_\beta D_\alpha^\dagger = \omega^{c(\alpha, \beta)} D_\beta$, for all $\alpha, \beta \in \mathbb{Z}_d \times \mathbb{Z}_d$.*

(iv). *$D_\alpha^\dagger = D_{-\alpha}$, for all $\alpha \in \mathbb{Z}_d \times \mathbb{Z}_d$.*

9

(v). $\operatorname{tr}(D_\alpha^\dagger D_\beta) = d \cdot \delta_{\alpha,\beta}$.

Proof. These properties are well-known (see e.g., [DPS04]) and can also be verified by direct calculation. The proof is omitted here. □

Lemma 3.4. *Define*

$$\rho := \frac{d}{d^2 + 1}\mathrm{id} + \frac{1}{2d(d^2+1)} \sum_{\beta \in \mathbb{Z}_d \times \mathbb{Z}_d} (D_\beta + D_\beta^\dagger).$$

Then ρ is a state, i.e., $\rho \in \mathrm{S}(\mathcal{H})$.

Proof. To show that the operator ρ is non-negative, we make use of the following operators. Let

$$
\begin{aligned}
|\psi_{km}^\nu\rangle &:= \frac{1}{\sqrt{2}}(\omega^{\frac{\nu}{2}}|k \oplus m\rangle + \omega^{-\frac{\nu}{2}}|m\rangle) && \text{and} \\
\rho_{km}^\nu &:= |\psi_{km}^\nu\rangle\langle\psi_{km}^\nu| && \text{for } \nu \in \mathbb{R}, k, m \in \mathbb{Z}_d, k \neq 0 \\
\rho_{0m}^\nu &:= (1 + \frac{\omega^\nu + \omega^{-\nu}}{2})|m\rangle\langle m|.
\end{aligned}
$$

Note that ρ_{0m}^ν is not normalized, but non-negative (it equals 0 if $(\nu \mod d) = \frac{d}{2}$).

With the definition

$$\nu(j,k,m) := \frac{j \odot k}{2} + jm ,$$

it is easy to verify that

$$\sum_m \rho_{km}^{\nu(j,k,m)} = \mathrm{id} + \frac{1}{2}(D_{jk} + D_{jk}^\dagger) ,$$

and hence

$$\rho = \frac{1}{d(d^2+1)} \sum_{j,k} \sum_m \rho_{km}^{\nu(j,k,m)} .$$

This implies that ρ is indeed positive. Let us show that ρ given by this expression is correctly normalized. Note that

$$
\begin{aligned}
\sum_{j,k,m} \operatorname{tr}\left(\rho_{km}^{\nu(j,k,m)}\right) &= \sum_{j,m}\sum_{k \neq 0} \operatorname{tr}\left(\rho_{km}^{\nu(j,k,m)}\right) + \sum_{j,m} \operatorname{tr}\left(\rho_{0m}^{\nu(j,0,m)}\right) \\
&= d^2(d-1) + \sum_{j,m}\left(1 + \frac{\omega^{\nu(j,0,m)} + \omega^{-\nu(j,0,m)}}{2}\right) .
\end{aligned}
$$

Because of

$$
\begin{aligned}
\sum_{j,m} \omega^{\nu(j,0,m)} &= \sum_{j,m} \omega^{jm} \\
&= d,
\end{aligned}
$$

where the second equation follows from (14), we obtain

$$\sum_{j,k,m} \operatorname{tr}\left(\rho_{km}^{\nu(j,k,m)}\right) = d(d^2 + 1). \tag{15}$$

This concludes the proof. □

Lemma 3.5. *Let*

$$\Delta_\alpha := \frac{1}{d^2+1}\mathrm{id} + \frac{1}{2d^2(d^2+1)} \sum_{\beta \in \mathbb{Z}_d \times \mathbb{Z}_d} (\omega^{c(\alpha,\beta)} D_\beta + \omega^{-c(\alpha,\beta)} D_\beta^\dagger).$$

Then $\mathfrak{Z} := \{\Delta_\alpha\}_{\alpha \in \mathbb{Z}_d \times \mathbb{Z}_d}$ is a POVM on $\mathcal{H}$.

10

Proof. We show that $\Delta_\alpha := \frac{1}{d} D_\alpha \rho D_\alpha^\dagger$ where $\rho \in S(\mathcal{H})$ is the state given in Lemma 3.4. The statement then follows from Lemma 3.3 (i) and (ii) because these imply that the operators are non-negative and resolve the identity.

We claim that

$$D_\alpha D_\beta^\dagger D_\alpha^\dagger = \omega^{-c(\alpha,\beta)} D_\beta^\dagger. \tag{16}$$

This can be verified as follows using the fact that the operators are unitary, Lemma 3.3 (iii), and the identity $c(\alpha,\beta) = -c(\beta,\alpha)$:

$$\begin{aligned}
D_\alpha D_\beta^\dagger D_\alpha^\dagger &= D_\beta^\dagger D_\beta D_\alpha D_\beta^\dagger D_\alpha^\dagger \\
&= D_\beta^\dagger \omega^{c(\beta,\alpha)} D_\alpha D_\alpha^\dagger \\
&= \omega^{-c(\alpha,\beta)} D_\beta^\dagger.
\end{aligned}$$

By inserting the state ρ given in Lemma 3.4, we obtain

$$\frac{1}{d} D_\alpha \rho D_\alpha^\dagger = \frac{1}{d^2+1} \mathrm{id} + \frac{1}{2d^2(d^2+1)} \sum_{\beta \in \mathbb{Z}_d \times \mathbb{Z}_d} (D_\alpha D_\beta D_\alpha^\dagger + D_\alpha D_\beta^\dagger D_\alpha^\dagger).$$

Using Lemma 3.3 (iii) again as well as the identity (16) establishes the fact that this equals Δ_α. $\qquad\square$

To simplify the notation, let us introduce the hermitian operators

$$\Lambda_\alpha := \frac{1}{2d} \sum_{\beta \in \mathbb{Z}_d \times \mathbb{Z}_d} (\omega^{c(\alpha,\beta)} D_\beta + \omega^{-c(\alpha,\beta)} D_\beta^\dagger).$$

With these operators, the POVM in question has the simple form

$$\Delta_\alpha := \frac{1}{d^2+1} \cdot \left(\mathrm{id} + \frac{1}{d} \cdot \Lambda_\alpha \right) \qquad \text{for all } \alpha \in \mathbb{Z}_d \times \mathbb{Z}_d. \tag{17}$$

Let us first compute two useful identities concerning the trace of these operators.

Lemma 3.6. *For all* $\alpha, \beta \in \mathbb{Z}_d \times \mathbb{Z}_d$

$$\begin{aligned}
\mathrm{tr}(\Lambda_\alpha) &= 1. \\
\mathrm{tr}(\Lambda_\alpha^\dagger \Lambda_\beta) &= d \cdot \delta_{\alpha,\beta}.
\end{aligned}$$

Proof. As $D_0 = \mathrm{id}$, we have from Lemma 3.3 (v) the identity $\mathrm{tr}(D_\beta) = d \cdot \delta_{\beta,0}$. With

$$\mathrm{tr}(A^\dagger) = \overline{\mathrm{tr}(A)} \tag{18}$$

this gives

$$\mathrm{tr}(\Lambda_\alpha) = \frac{1}{2}(\omega^{c(\alpha,0)} + \omega^{-c(\alpha,0)}) = 1 .$$

Because of

$$\Lambda_\alpha^\dagger \Lambda_\beta = \frac{1}{4d^2} \left(\sum_\gamma \omega^{-c(\alpha,\gamma)} D_\gamma^\dagger + \omega^{c(\alpha,\gamma)} D_\gamma \right) \left(\sum_\delta \omega^{c(\beta,\delta)} D_\delta + \omega^{-c(\beta,\delta)} D_\delta^\dagger \right)$$

and identity (18) we have

$$\mathrm{tr}(\Lambda_\alpha^\dagger \Lambda_\beta) = \frac{1}{4d^2} \sum_{\gamma,\delta} \left(\omega^{c(\beta,\delta)-c(\alpha,\gamma)} \mathrm{tr}(D_\gamma^\dagger D_\delta) + \omega^{c(\alpha,\gamma)+c(\beta,\delta)} \mathrm{tr}(D_\gamma D_\delta) \right) \qquad + \quad h.c.,$$

where $h.c.$ denotes the complex conjugate of the previous expression. Applying Lemma 3.3 (iv) and (v) gives

$$\mathrm{tr}(\Lambda_\alpha^\dagger \Lambda_\beta) = \frac{1}{4d} \cdot \sum_\gamma \left(\omega^{c(\beta,\gamma)-c(\alpha,\gamma)} + \omega^{c(\alpha,\gamma)+c(\beta,-\gamma)} \right) \quad + \quad h.c.$$

But $c(\beta,-\gamma) = -c(\beta,\gamma)$ and $c(\beta,\gamma) - c(\alpha,\gamma) = c(\beta-\alpha,\gamma)$, hence we obtain

$$\mathrm{tr}(\Lambda_\alpha^\dagger \Lambda_\beta) = \frac{1}{4d} \cdot \sum_\gamma (\omega^{c(\beta-\alpha,\gamma)} + \omega^{c(\alpha-\beta,\gamma)}) \quad + \quad h.c.$$

and thus finally

$$\mathrm{tr}(\Lambda_\alpha^\dagger \Lambda_\beta) = d \cdot \delta_{\alpha,\beta},$$

as a consequence of equation (13). $\qquad\square$

Lemma 3.7. *The POVM $\mathfrak{Z}$ is a dual of the family of hermitian operators*

$$\Theta_\alpha := -d\left(\mathrm{id} - \frac{d^2+1}{d} \cdot \Lambda_\alpha\right) \qquad \alpha \in \mathbb{Z}_d \times \mathbb{Z}_d.$$

Proof. The operators Θ_α are hermitian since, by definition, the operators Λ_α are hermitian. The fact that $\mathfrak{Z}$ is a dual of the family of operators Θ_α follows from the representation (17) of the POVM operators and Lemma 3.6. $\qquad\square$

Lemma 3.8. *For every $\alpha \in \mathbb{Z}_d \times \mathbb{Z}_d$, $\mathrm{tr}(|\Theta_\alpha|) \le d \cdot \sqrt{d^4 + d^2 - 1}$.*

Proof. Let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of Θ_α (including multiplicities). Then

$$\begin{aligned}
\mathrm{tr}(|\Theta_\alpha|) &= \sum_{i=1}^d |\lambda_i| \\
&\le d^{\frac{1}{2}} \sqrt{\sum_{i=1}^d |\lambda_i|^2} \\
&= d^{\frac{1}{2}} \sqrt{\mathrm{tr}(\Theta_\alpha^\dagger \Theta_\alpha)}.
\end{aligned}$$

But $\mathrm{tr}(\Theta_\alpha^\dagger \Theta_\alpha) = d(d^4 + d^2 - 1)$ as can be computed directly using Lemma 3.6. $\qquad\square$

4 Analysis of symmetric probability distributions

In this section, we derive a number of useful properties of symmetric probability distributions. These results will later be applied to probability distributions resulting from measurements of a symmetric quantum state.

It is worth noting that our proof of the finite quantum de Finetti representation does not rely on a classical de Finetti-style theorem (as opposed to [CFS02]). It is, however, straightforward to obtain a de Finetti representation for (classical) probability distributions based on the results presented in the sequel.

4.1 Estimating the frequency distribution of a subsequence

Let $(\mathbf{z}, \bar{\mathbf{z}})$ be the concatenation of an n-tuple $\mathbf{z}$ and a k-tuple $\bar{\mathbf{z}}$ of elements from $\mathcal{Z}$. We show that, if $(\mathbf{z}, \bar{\mathbf{z}})$ is randomly chosen according to a symmetric probability distribution $P_{(\mathbf{z},\bar{\mathbf{z}})}$, then the frequency distribution $Q_{\bar{\mathbf{z}}}$ of the sub-tuple $\bar{\mathbf{z}}$ is a good estimate for the frequency distribution $Q_{\mathbf{z}}$ of the remaining subsequence $\mathbf{z}$.

We need the following simple relation between the distances of frequency distributions of subsequences obtained from a sequence of elements from $\mathcal{Z}$.

Lemma 4.1. *Let $\mathcal{Z}$ be a set and let $\mathbf{z}$ and $\bar{\mathbf{z}}$ be elements of $\mathcal{Z}^n$ and $\mathcal{Z}^k$, respectively. Then*

$$\delta(Q_{\mathbf{z}}, Q_{\bar{\mathbf{z}}}) \leq \frac{n+k}{n} \delta(Q_{\bar{\mathbf{z}}}, Q_{(\mathbf{z},\bar{\mathbf{z}})}) \ .$$

Proof. By the definition of the frequency distribution,

$$(n+k)Q_{(\mathbf{z},\bar{\mathbf{z}})} = nQ_{\mathbf{z}} + kQ_{\bar{\mathbf{z}}} \ .$$

Hence, using the convexity of the variational distance,

$$\delta(Q_{(\mathbf{z},\bar{\mathbf{z}})}, Q_{\mathbf{z}}) = \delta\left(\frac{n}{n+k}Q_{\mathbf{z}} + \frac{k}{n+k}Q_{\bar{\mathbf{z}}}, Q_{\mathbf{z}}\right) \leq \frac{k}{n+k} \delta(Q_{\bar{\mathbf{z}}}, Q_{\mathbf{z}}) \ .$$

The triangle inequality then leads to

$$\delta(Q_{\bar{\mathbf{z}}}, Q_{\mathbf{z}}) \leq \delta(Q_{\bar{\mathbf{z}}}, Q_{(\mathbf{z},\bar{\mathbf{z}})}) + \delta(Q_{(\mathbf{z},\bar{\mathbf{z}})}, Q_{\mathbf{z}}) \leq \delta(Q_{\bar{\mathbf{z}}}, Q_{(\mathbf{z},\bar{\mathbf{z}})}) + \frac{k}{n+k} \delta(Q_{\bar{\mathbf{z}}}, Q_{\mathbf{z}}) \ ,$$

from which the assertion follows. $\qquad\square$

We now show that $Q_{\mathbf{z}}$ is close to $Q_{\bar{\mathbf{z}}}$ by showing that the expression on the r.h.s. of the inequality in Lemma 4.1 is small in expectation.

Lemma 4.2. *Let $\mathbf{Z}$ be an n-tuple and $\bar{\mathbf{Z}}$ a k-tuple of random variables over a set $\mathcal{Z}$ of size $|\mathcal{Z}| = t$ such that $P_{(\mathbf{Z},\bar{\mathbf{Z}})}$ is symmetric. Then, for $(\mathbf{z},\bar{\mathbf{z}}) \leftarrow P_{(\mathbf{Z},\bar{\mathbf{Z}})}$,*

$$\mathop{\mathbb{E}}_{(\mathbf{z},\bar{\mathbf{z}})}[\delta(Q_{\bar{\mathbf{z}}}, Q_{(\mathbf{z},\bar{\mathbf{z}})})] \leq \frac{1}{2}\sqrt{\frac{t}{k}} \ .$$

Proof. Let $\mathbf{Z} := (Z_1, \dots, Z_n)$ and $\bar{\mathbf{Z}} := (\bar{Z}_1, \dots, \bar{Z}_k)$. It suffices to show that, for all probability distributions $q \in \mathrm{Distr}(\mathcal{Z})$,

$$\mathop{\mathbb{E}}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}}[\delta(Q_{\bar{\mathbf{z}}}, q)] \leq \frac{1}{2}\sqrt{\frac{t}{k}} \tag{19}$$

The assertion then follows from

$$\mathop{\mathbb{E}}_{(\mathbf{z},\bar{\mathbf{z}}) \leftarrow P_{(\mathbf{Z},\bar{\mathbf{Z}})}}[\delta(Q_{\bar{\mathbf{z}}}, Q_{(\mathbf{z},\bar{\mathbf{z}})})] = \mathop{\mathbb{E}}_{q \leftarrow P_{Q_{(\mathbf{Z},\bar{\mathbf{Z}})}}}\left[\mathop{\mathbb{E}}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}}[\delta(Q_{\bar{\mathbf{z}}}, q)]\right] \ .$$

Let thus $q \in \mathrm{Distr}(\mathcal{Z})$ be fixed. For every $z \in \mathcal{Z}$, let χ_z be the function on $\mathcal{Z}$ defined by $\chi_z(z') = 1$ if $z' = z$ and $\chi_z(z') = 0$ otherwise. Then

$$\delta(Q_{\bar{\mathbf{z}}}, q) = \frac{1}{2}\sum_{z \in \mathcal{Z}}|d_z(\bar{\mathbf{z}})| \tag{20}$$

where, for any $\bar{\mathbf{z}} = (\bar{z}_1, \dots, \bar{z}_k) \in \mathcal{Z}^k$,

$$d_z(\bar{\mathbf{z}}) := \frac{1}{k}\sum_{i=1}^{k}\left(\chi_z(\bar{z}_i) - q(z)\right) \ .$$

Using Jensen's inequality,

$$\mathop{\mathbb{E}}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}}\left[|d_z(\bar{\mathbf{z}})|\right] \leq \sqrt{\mathop{\mathbb{E}}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}}\left[d_z(\bar{\mathbf{z}})^2\right]} \tag{21}$$

We claim that for any $i \neq j$,

$$\mathop{\mathbb{E}}_{(\bar{z}_i,\bar{z}_j) \leftarrow P_{(\bar{Z}_i,\bar{Z}_j)|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}}\left[(\chi_z(\bar{z}_i) - q(z))(\chi_z(\bar{z}_j) - q(z))\right] \leq 0 \ . \tag{22}$$

To prove this identity, first note that the expectation value can be written in the form

$$\mathbb{E}_{\bar{z}_i \leftarrow P_{\bar{Z}_i|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}} \left[\mathbb{E}_{\bar{z}_j \leftarrow P_{\bar{Z}_j|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q, \bar{Z}_i = \bar{z}_i}} \left[(\chi_z(\bar{z}_i) - q(z))(\chi_z(\bar{z}_j) - q(z)) \right] \right].$$

Since $0 \leq q(z) \leq 1$, it suffices to show that

$$\mathbb{E}_{\bar{z}_j \leftarrow P_{\bar{Z}_j|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q, \bar{Z}_i = \bar{z}_i}} \left[\chi_z(\bar{z}_j) - q(z) \right] \begin{cases} \leq 0 & \text{if } \bar{z}_i = z \\ \geq 0 & \text{otherwise.} \end{cases} \tag{23}$$

Because of Lemma 2.3, the probability distribution $P_{\bar{Z}_j|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q, \bar{Z}_i = \bar{z}_i}$ is symmetric. Hence by the definition of the frequency distribution, we have

$$\mathbb{E}_{\bar{z}_j \leftarrow P_{\bar{Z}_j|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q, \bar{Z}_i = \bar{z}_i}} \left[\chi_z(\bar{z}_j) \right] = P_{\bar{Z}_j|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q, \bar{Z}_i = \bar{z}_i}(z) = \begin{cases} \frac{nq(z)-1}{n-1} & \text{if } z = \bar{z}_i \\ \frac{nq(z)}{n-1} & \text{otherwise.} \end{cases}$$

This proves (23) and thus (22).

Using (22) and Lemma 2.4, we obtain

$$\mathbb{E}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}} \left[d_z(\bar{\mathbf{z}})^2 \right] \leq \frac{1}{k^2} \sum_{i=1}^{k} \mathbb{E}_{\bar{z}_i \leftarrow P_{\bar{Z}_i|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}} \left[(\chi_z(\bar{z}_i) - q(z))^2 \right]$$

$$= \frac{1}{k^2} \sum_{i=1}^{k} \left(q(z) - q(z)^2 \right) \leq \frac{q(z)}{k} . \tag{24}$$

Combining (20), (21), and (24) leads to

$$\mathbb{E}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}} \left[\delta(Q_{\bar{\mathbf{z}}}, q) \right] = \frac{1}{2} \sum_{z \in \mathcal{Z}} \sqrt{\frac{q(z)}{k}} .$$

The bound (19) then follows from Jensen's inequality, which concludes the proof. $\qquad\square$

4.2 The product structure of symmetric probability distributions

Let $\mathbf{z}$ be an n-tuple over $\mathcal{Z}$ randomly chosen according to a probability distribution $P_{\mathbf{Z}}$ and let $q \in \text{Distr}(\mathcal{Z})$ be an estimate for the frequency distribution $Q_{\mathbf{z}}$ of $\mathbf{z}$. To quantify the quality of this estimate, it is convenient to introduce the abbreviation $D_q(P_{\mathbf{Z}})$ for the expected distance between the actual frequency distribution $Q_{\mathbf{z}}$ and the estimate q, that is

$$D_q(P_{\mathbf{Z}}) := \mathbb{E}_{\mathbf{z} \leftarrow P_{\mathbf{Z}}} [\delta(Q_{\mathbf{z}}, q)] .$$

The main result of Section 4.1 can then be rephrased as follows.

Lemma 4.3. *Let $\mathbf{Z}$ be an n-tuple and $\bar{\mathbf{Z}}$ a k-tuple of random variables over a set $\mathcal{Z}$ of size $|\mathcal{Z}| = t$, for $k \leq n$, such that $P_{(\mathbf{Z},\bar{\mathbf{Z}})}$ is symmetric. Then, for $\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}}$,*

$$\mathbb{E}_{\bar{\mathbf{z}}}[D_{Q_{\bar{\mathbf{z}}}}(P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}})] \leq \sqrt{\frac{t}{k}} .$$

Proof. From Lemma 4.2 and Lemma 4.1,

$$\mathbb{E}_{(\mathbf{z},\bar{\mathbf{z}}) \leftarrow P_{(\mathbf{Z},\bar{\mathbf{Z}})}} [\delta(Q_{\mathbf{z}}, Q_{\bar{\mathbf{z}}})] \leq \sqrt{\frac{t}{k}}$$

The assertion then follows from the definition of $D_{\cdot}(\cdot)$. $\qquad\square$

Lemma 4.4 establishes a connection between the quantity $D_q(P_{\mathbf{Z}})$ and the product structure of symmetric probability distributions.

Lemma 4.4. *Let Y be a random variable over $\mathcal{Y}$ and let $\mathbf{Z} = (Z_1, \ldots, Z_r)$ be an r-tuple of random variables over $\mathcal{Z}$, such that the conditional probability distribution $P_{\mathbf{Z}|Y=y}$ is symmetric for every $y \in \mathcal{Y}$. Then, for all $q \in \mathrm{Distr}(\mathcal{Z})$,*

$$\delta(P_{YZ_i}, P_Y \times q) \leq D_q(P_{\mathbf{Z}}) , \quad \text{for every } i \in [r].$$

Proof. Using the strong convexity of the variational distance, we have

$$\delta(P_{YZ_i}, P_Y \times q) \leq \mathop{\mathbb{E}}_{\tilde{q} \leftarrow P_{Q_{\mathbf{Z}}}} \left[\delta(P_{YZ_i|Q_{\mathbf{Z}}=\tilde{q}}, P_{Y|Q_{\mathbf{Z}}=\tilde{q}} \times q) \right] . \tag{25}$$

Since $P_{\mathbf{Z}|Y=y}$ is symmetric, Lemma 2.4 implies $P_{Z_i|Y=y,Q_{\mathbf{Z}}=\tilde{q}} = \tilde{q}$, for every $y \in \mathcal{Y}$. Hence,

$$\delta(P_{YZ_i|Q_{\mathbf{Z}}=\tilde{q}}, P_{Y|Q_{\mathbf{Z}}=\tilde{q}} \times q) = \delta(P_{Y|Q_{\mathbf{Z}}=\tilde{q}} \times \tilde{q}, P_{Y|Q_{\mathbf{Z}}=\tilde{q}} \times q) = \delta(\tilde{q}, q) \tag{26}$$

where the last equality follows from (4). Combining (25) and (26) leads to

$$\delta(P_{YZ_i}, P_Y \times q) \leq \mathop{\mathbb{E}}_{\tilde{q} \leftarrow P_{Q_{\mathbf{Z}}}} \left[\delta(\tilde{q}, q) \right] = \mathop{\mathbb{E}}_{\mathbf{z} \leftarrow P_{\mathbf{Z}}} \left[\delta(Q_{\mathbf{z}}, q) \right] = D_q(P_{\mathbf{Z}}) .$$

$\square$

5 Analysis of symmetric quantum states

The goal of this section is to derive results on symmetric quantum states, based on the corresponding results of symmetric probability distribution given in the previous section. In Section 5.1, we first show how certain properties of the measurement statistics imply structural properties of the corresponding quantum states. Then, in Section 5.2, we combine these results with those of Section 4.2 in order to prove statements about the structure of symmetric quantum states.

5.1 Deducing the state structure from measurement results

Consider a state of a bipartite system conditioned on a measurement on one of the systems. We first prove an upper bound on the amount of dependence between this conditional state and the measurement outcome.

Lemma 5.1. *Let $\rho^{AB} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}_B$. Then, for all $q \in \mathrm{Distr}(\mathcal{Z})$ and $z \in \mathcal{Z}$,*

$$\delta(\rho^A_{|\mathfrak{Z}=z}, \rho^A) \leq \frac{2}{\rho^B_{\mathfrak{Z}}(z)} \max_{\mathfrak{Y}} \delta(\rho^{AB}_{\mathfrak{Y}\mathfrak{Z}}, \rho^A_{\mathfrak{Y}} \times q) ,$$

where the maximization is over all POVMs $\mathfrak{Y}$ on $\mathcal{H}_A$.

Proof. Let $\mathfrak{Y} := \{E_y\}_{y \in \mathcal{Y}}$ be a POVM on $\mathcal{H}_A$. Then, from the triangle inequality, (2) and (4),

$$\begin{aligned} \delta(\rho^{AB}_{\mathfrak{Y}\mathfrak{Z}}, \rho^A_{\mathfrak{Y}} \times \rho^B_{\mathfrak{Z}}) &\leq \delta(\rho^{AB}_{\mathfrak{Y}\mathfrak{Z}}, \rho^A_{\mathfrak{Y}} \times q) + \delta(\rho^A_{\mathfrak{Y}} \times q, \rho^A_{\mathfrak{Y}} \times \rho^B_{\mathfrak{Z}}) \\ &= \delta(\rho^{AB}_{\mathfrak{Y}\mathfrak{Z}}, \rho^A_{\mathfrak{Y}} \times q) + \delta(q, \rho^B_{\mathfrak{Z}}) \\ &\leq 2D \end{aligned} \tag{27}$$

where

$$D := \max_{\mathfrak{Y}} \delta(\rho^{AB}_{\mathfrak{Y}\mathfrak{Z}}, \rho^A_{\mathfrak{Y}} \times q) ,$$

with the maximization ranging over all POVMs $\mathfrak{Y}$ on $\mathcal{H}_A$. Using equation (3), we have

$$\rho_{\mathfrak{Z}}^B(z) \cdot \delta\big(\rho_{\mathfrak{Y}|\mathfrak{Z}=z}^A, \rho_{\mathfrak{Y}}^A\big) \leq \mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \big[\delta\big(\rho_{\mathfrak{Y}|\mathfrak{Z}=z}^A, \rho_{\mathfrak{Y}}^A\big)\big] = \delta(\rho_{\mathfrak{Y}\mathfrak{Z}}^{AB}, \rho_{\mathfrak{Y}}^A \times \rho_{\mathfrak{Z}}^B) \ .$$

With (27), it follows that

$$\delta\big(\rho_{\mathfrak{Y}|\mathfrak{Z}=z}^A, \rho_{\mathfrak{Y}}^A\big) \leq \frac{2D}{\rho_{\mathfrak{Z}}^B(z)}$$

for every $z \in \mathcal{Z}$ and every POVM $\mathfrak{Y}$ on $\mathcal{H}_A$. Therefore, using (8), we conclude that

$$\delta(\rho^A|\mathfrak{Z}=z, \rho^A) = \max_{\mathfrak{Y}} \delta\big(\rho_{\mathfrak{Y}|\mathfrak{Z}=z}^A, \rho_{\mathfrak{Y}}^A\big) \leq \frac{2D}{\rho_{\mathfrak{Z}}^B(z)} \ . \qquad \square$$

For a POVM $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ on a Hilbert space $\mathcal{H}$, we define the constants

$$
\begin{aligned}
C_1(\mathfrak{Z}) &:= \min_{\{F_z^*\}_{z \in \mathcal{Z}}} 2 \cdot \left(\sum_{z \in \mathcal{Z}} \mathrm{tr}(|F_z^*|)\right) \\
C_2(\mathfrak{Z}) &:= \sqrt{|\mathcal{Z}|} \cdot C_1(\mathfrak{Z}).
\end{aligned}
$$

where the minimum ranges over all families $\{F_z^*\}_{z \in \mathcal{Z}}$ of elements from $\mathrm{Herm}(\mathcal{H})$ such that $\mathfrak{Z}$ is the dual of $\{F_z^*\}_{z \in \mathcal{Z}}$. If no such family $\{F_z^*\}_{z \in \mathcal{Z}}$ exists, we set $C_1(\mathfrak{Z}) := \infty$.

Note that, due to Lemma 2.9, if $\mathfrak{Z}$ is an informationally complete POVM, then $\bar{C}_i(\mathfrak{Z}) < \infty$, for $i = 1, 2$. By the interpretation given to the values $\mathrm{tr}(|F_z^*|)$ in Section 2.4, the value $C_1(\mathfrak{Z})$ can be seen as a measure for the accuracy by which an unknown state ρ can be estimated from the statistics obtained by the measurement $\mathfrak{Z}$.

For a d-dimensional Hilbert space $\mathcal{H}$, let $\bar{C}_i(d)$ be the minimum of $C_i(\mathfrak{Z})$, minimized over all POVMs $\mathfrak{Z}$ on $\mathcal{H}$, that is

$$\bar{C}_i(d) := \min_{\mathfrak{Z}} C_i(\mathfrak{Z}) \ , \qquad \text{for } i = 1, 2 \ .$$

The following corollary is a direct consequence of of Lemma 3.2 and Lemma 3.8.

Corollary 5.2. *Let $\mathcal{H}$ be a d-dimensional Hilbert space. Then*

$$\bar{C}_1(d) \leq 2\sqrt{2} \cdot d^5 \ .$$
$$\bar{C}_2(d) \leq 2\sqrt{2} \cdot d^6 \ .$$

If symmetric informationally complete POVMs exist in dimension d, then

$$\bar{C}_1(d) \leq 2d^2(2d-1) \ .$$
$$\bar{C}_2(d) \leq 2d^3(2d-1) \ .$$

The main result of this section expresses the intuitive fact that a bipartite state has product form if every bipartite measurement yields a product distribution.

Theorem 5.3. *Let $\rho^{AB} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and let $\mathfrak{Z}$ be a POVM on $\mathcal{H}_B$. Then, for any $q \in \mathrm{Distr}(\mathcal{Z})$,*

$$\delta(\rho^{AB}, \rho^A \otimes \rho^B) \leq C_1(\mathfrak{Z}) \cdot \max_{\mathfrak{Y}} \delta(\rho_{\mathfrak{Y}\mathfrak{Z}}^{AB}, \rho_{\mathfrak{Y}}^A \times q) \ .$$

In particular, if $\mathcal{H}_B$ is d-dimensional, then

$$\delta(\rho^{AB}, \rho^A \otimes \rho^B) \leq \bar{C}_1(d) \cdot \max_{\mathfrak{Y},\mathfrak{Z}} \delta(\rho_{\mathfrak{Y}\mathfrak{Z}}^{AB}, \rho_{\mathfrak{Y}}^A \times \rho_{\mathfrak{Z}}^B) \ .$$

(The maxima are taken over all POVMs $\mathfrak{Y}$ on $\mathcal{H}_A$ and $\mathfrak{Z}$ on $\mathcal{H}_B$, respectively.)

Proof. Let $\{F_z^*\}_{z \in \mathcal{Z}}$ be a family of elements from $\mathrm{Herm}(\mathcal{H}_B)$ such that $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ is the dual of $\{F_z^*\}_{z \in \mathcal{Z}}$. Then, according to (11),

$$\rho^{AB} = \mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \left[\rho^A{}_{|\mathfrak{Z}=z} \otimes F_z^* \right] \qquad \text{and} \qquad \rho^B = \mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \left[F_z^* \right] .$$

Using these identities, the strong convexity of the trace distance, and Lemma 2.1, we obtain

$$\begin{aligned}
\delta(\rho^{AB}, \rho^A \otimes \rho^B) &= \delta\big(\mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \left[\rho^A{}_{|\mathfrak{Z}=z} \otimes F_z^* \right], \mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \left[\rho^A \otimes F_z^* \right]\big) \\
&\leq \mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \left[\delta(\rho^A{}_{|\mathfrak{Z}=z} \otimes F_z^*, \rho^A \otimes F_z^*) \right] \\
&= \mathop{\mathbb{E}}_{z \leftarrow \rho_{\mathfrak{Z}}^B} \left[\delta(\rho^A{}_{|\mathfrak{Z}=z}, \rho^A) \cdot \mathrm{tr}(|F_z^*|) \right] .
\end{aligned}$$

The assertion then follows from Lemma 5.1 and the definition of $C_1(\mathfrak{Z})$. $\qquad\square$

5.2 The product structure of symmetric quantum states

We now combine the results of Section 4 and Section 5.1. We start with a quantum analogue of Lemma 4.4.

Lemma 5.4. *Let $\rho^{A\overline{r}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes r})$ be symmetric relative to $\mathcal{H}_A$ and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}$. Then, for any $q \in \mathrm{Distr}(\mathcal{Z})$,*

$$\delta(\rho^{A\overline{1}}, \rho^A \otimes \rho^{\overline{1}}) \leq C_1(\mathfrak{Z}) \, D_q(\rho_{\mathfrak{Z}^r}^{\overline{r}})$$

and

$$\delta(\rho_{\mathfrak{Z}}^{\overline{1}}, q) \leq D_q(\rho_{\mathfrak{Z}^r}^{\overline{r}}) .$$

Proof. Let $\mathfrak{Y}$ be a POVM on $\mathcal{H}_A$. Since, by Lemma 2.6, $\rho^{\overline{r}}{}_{|\mathfrak{Y}=y}$ is symmetric, the probability distribution $\rho_{\mathfrak{Z}^r|\mathfrak{Y}=y}^{\overline{r}}$ is also symmetric, for all $y \in \mathcal{Y}$. Lemma 4.4 thus implies

$$\delta(\rho_{\mathfrak{Y}\mathfrak{Z}}^{A\overline{1}}, \rho_{\mathfrak{Y}}^A \times q) \leq D_q(\rho_{\mathfrak{Z}^r}^{\overline{r}}) . \tag{28}$$

The first assertion of the lemma then follows from Theorem 5.3.

The second assertion of the lemma follows directly from (28) and property (2) of the variational distance, i.e., $\delta(\rho_{\mathfrak{Z}}^{\overline{1}}, q) \leq \delta(\rho_{\mathfrak{Y}\mathfrak{Z}}^{A\overline{1}}, \rho_{\mathfrak{Y}}^A \times q)$. $\qquad\square$

The next lemma shows that symmetry imposes severe constraints on the structure of quantum states. More precisely, if a symmetric quantum state has product structure with respect to one of its subsystems, this directly implies that the state has product structure with respect to all its subsystems.

Lemma 5.5. *Let $\rho^{A\overline{n}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n})$ be symmetric relative to $\mathcal{H}_A$. Then*

$$\delta(\rho^{A\overline{n}}, \rho^A \otimes (\rho^{\overline{1}})^{\otimes n}) \leq n \cdot \delta(\rho^{A\overline{n}}, \rho^{A\overline{n-1}} \otimes \rho^{\overline{1}}) .$$

Proof. Using the triangle inequality for the trace distance, we get

$$\delta(\rho^{A\overline{n}}, \rho^A \otimes (\rho^{\overline{1}})^{\otimes n}) \leq \sum_{i=0}^{n-1} \delta(\rho^{A\overline{n-i}} \otimes (\rho^{\overline{1}})^{\otimes i}, \rho^{A\overline{n-i-1}} \otimes (\rho^{\overline{1}})^{\otimes(i+1)}). \tag{29}$$

Since, by equation (7), the trace distance does not change when tracing out the product state $(\rho^{\overline{1}})^{\otimes i}$, we have, for any $i \in [n]$,

$$\delta(\rho^{A\overline{n-i}} \otimes (\rho^{\overline{1}})^{\otimes i}, \rho^{A\overline{n-i-1}} \otimes (\rho^{\overline{1}})^{\otimes(i+1)}) = \delta\big(\rho^{A\overline{n-i}}, \rho^{A\overline{n-i-1}} \otimes \rho^{\overline{1}}\big) . \tag{30}$$

Using the fact that the trace distance can only decrease when taking a partial trace (see (5)), we get

$$\delta(\rho^{A\overline{n-i}}, \rho^{A\overline{n-i-1}} \otimes \rho^{\overline{1}}) \le \delta(\rho^{A\overline{n}}, \rho^{A\overline{n-1}} \otimes \rho^{\overline{1}}) \ . \tag{31}$$

Combining (30) with (31) and inserting this into (29) concludes the proof. $\square$

Combined with Lemma 5.4, we obtain an upper bound on the distance between a symmetric state with n subsystems and an n-fold product state.

Corollary 5.6. *Let $\rho^{A\overline{n+m}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n+m})$ be symmetric relative to $\mathcal{H}_A$ and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}$. Then, for any $q \in \mathrm{Distr}(\mathcal{Z})$,*

$$\delta(\rho^{A\overline{n}}, \rho^A \otimes (\rho^{\overline{1}})^{\otimes n}) \le n \, C_1(\mathfrak{Z}) \, D_q(\rho_{\mathfrak{Z}^{m+1}}^{\overline{m+1}}) \ .$$

Proof. Obviously, the density operator $\rho^{A\overline{n+m}}$ is symmetric relative to $\mathcal{H}_{A'} := \mathcal{H}_A \otimes \mathcal{H}^{\otimes n-1}$. Thus, with $r := m + 1$, we can write $\rho^{A'\overline{r}}$ instead of $\rho^{A\overline{n+m}}$, and, similarly, $\rho^{A\overline{n}} = \rho^{A'\overline{1}}$ and $\rho^{A\overline{n-1}} = \rho^{A'}$. Hence, by Lemma 5.4,

$$\delta(\rho^{A\overline{n}}, \rho^{A\overline{n-1}} \otimes \rho^{\overline{1}}) = \delta(\rho^{A'\overline{1}}, \rho^{A'} \otimes \rho^{\overline{1}}) \le C_1(\mathfrak{Z}) \, D_q(\rho_{\mathfrak{Z}^r}^{\overline{r}}) \ .$$

Applying Lemma 5.5 concludes the proof. $\square$

Finally, we give an upper bound on the expected value of the quantity appearing on the r.h.s. in Corollary 5.6. For this, we need a quantum analogue of Lemma 4.3.

Lemma 5.7. *Let $\rho^{\overline{n+k}} \in \mathrm{S}(\mathcal{H}^{\otimes n+k})$, for $k \le n$, be symmetric and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}$ with $|\mathcal{Z}| = t$. Then, for $\bar{\mathbf{z}} \leftarrow \rho_{\mathfrak{Z}^k}^{\overline{k}}$,*

$$\mathbb{E}_{\bar{\mathbf{z}}}\big[D_{Q_{\bar{\mathbf{z}}}}(\rho_{\mathfrak{Z}^n|\mathfrak{Z}^k=\bar{\mathbf{z}}}^{\overline{n}})\big] \le \sqrt{\frac{t}{k}} \ .$$

Proof. The assertion follows directly from Lemma 4.3 and the fact that the probability distribution $\rho_{\mathfrak{Z}^n\mathfrak{Z}^k}^{\overline{n}\,\overline{k}}$ is symmetric. $\square$

6 Main results

Our main results immediately follow from the characterizations of symmetric quantum states given in the preceding section. Basically, we consider the quantum state $\rho_{\bar{\mathbf{z}}}^{A\overline{n}} := \rho^{A\overline{n}}{}_{|\mathfrak{Z}^k=\bar{\mathbf{z}}}$ on $\mathcal{H}_A \otimes \mathcal{H}^{\otimes n}$ obtained by conditioning an exchangeable state $\rho^{A\overline{n+k}}$ on the outcomes $\bar{\mathbf{z}} = (z_1, \ldots, z_k)$ of a POVM $\mathfrak{Z}$ applied to k subsystems $\mathcal{H}$. We show that $\rho_{\bar{\mathbf{z}}}^{A\overline{n}}$ is close to a product state $\rho_{\bar{\mathbf{z}}}^A \otimes (\rho_{\bar{\mathbf{z}}}^{\overline{1}})^{\otimes n}$ where $\rho_{\bar{\mathbf{z}}}^{\overline{1}}$ is a density operator on a single subsystem $\mathcal{H}$. Moreover, $\rho_{\bar{\mathbf{z}}}^{\overline{1}}$ is almost determined by the observed measurement statistics.

Theorem 6.1. *Let $\rho^{A\overline{n+k}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n+k})$ be $(n + 2k - 1)$-exchangeable relative to $\mathcal{H}_A$ and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}$ with $|\mathcal{Z}| = t$. For every $\bar{\mathbf{z}} \in \mathcal{Z}^k$, let $\rho_{\bar{\mathbf{z}}}^{A\overline{n}} := \rho^{A\overline{n}}{}_{|\mathfrak{Z}^k=\bar{\mathbf{z}}}$. Then for $\bar{\mathbf{z}} \leftarrow \rho_{\mathfrak{Z}^k}^{\overline{k}}$*

$$\mathbb{E}_{\bar{\mathbf{z}}}\Big[\delta\big(\rho_{\bar{\mathbf{z}}}^{A\overline{n}}, \rho_{\bar{\mathbf{z}}}^A \otimes (\rho_{\bar{\mathbf{z}}}^{\overline{1}})^{\otimes n}\big)\Big] \le C_2(\mathfrak{Z}) \, \frac{n}{\sqrt{k}}$$

where $\rho_{\bar{\mathbf{z}}}^{\overline{1}} = \rho^{\overline{1}}{}_{|\mathfrak{Z}^k=\bar{\mathbf{z}}}$ is determined by

$$\mathbb{E}_{\bar{\mathbf{z}}}\Big[\delta\big(\rho_{\mathfrak{Z}|\mathfrak{Z}^k=\bar{\mathbf{z}}}^{\overline{1}}, Q_{\bar{\mathbf{z}}}\big)\Big] \le \sqrt{\frac{t}{k}} \ .$$

Proof. Let $m := k - 1$. According to the definition of exchangeability, there exists an extension $\rho^{A\overline{n+k+m}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n+k+m})$ of $\rho^{A\overline{n+k}}$ which is symmetric relative to $\mathcal{H}_A$. For every $\bar{\mathbf{z}} \in \mathcal{Z}^k$, let $[\rho_{\bar{\mathbf{z}}}]^{A\overline{n+m}} := \rho^{A\overline{n+m}}_{|\mathfrak{Z}^k = \bar{\mathbf{z}}}$.

By Lemma 2.6, $[\rho_{\bar{\mathbf{z}}}]^{A\overline{n+m}}$ is symmetric relative to $\mathcal{H}_A$. Hence, from the second bound of Lemma 5.4, with $r := m + 1$,

$$\delta([\rho_{\bar{\mathbf{z}}}]^{\overline{1}}_{\mathfrak{Z}}, Q_{\bar{\mathbf{z}}}) \leq D_{Q_{\bar{\mathbf{z}}}}([\rho_{\bar{\mathbf{z}}}]^{\overline{m+1}}_{\mathfrak{Z}^{m+1}}) \tag{32}$$

and, from Corollary 5.6,

$$\delta([\rho_{\bar{\mathbf{z}}}]^{A\overline{n}}, [\rho_{\bar{\mathbf{z}}}]^A \otimes ([\rho_{\bar{\mathbf{z}}}]^{\overline{1}})^{\otimes n}) \leq n\, C_1(\mathfrak{Z})\, D_{Q_{\bar{\mathbf{z}}}}([\rho_{\bar{\mathbf{z}}}]^{\overline{m+1}}_{\mathfrak{Z}^{m+1}}) \ . \tag{33}$$

Since $k = m + 1$, we can apply Lemma 5.7 to the state $\rho^{\overline{(m+1)+k}}$, i.e.,

$$\mathbb{E}_{\bar{\mathbf{z}}}\big[D_{Q_{\bar{\mathbf{z}}}}([\rho_{\bar{\mathbf{z}}}]^{\overline{m+1}}_{\mathfrak{Z}^{m+1}})\big] \leq \sqrt{\frac{t}{k}} \ .$$

The assertion follows by taking the expectation on both sides of (32) and (33), respectively. $\square$

Using Markov's inequality, it is straightforward to turn Theorem 6.1, which expresses closeness in terms of expected distance, into a statement providing a bound on the probability that the distance is larger than a given value ε. However, by adapting the auxiliary results derived so far and using a tail inequality by Hoeffding, we obtain a tighter bound. The interested reader is referred to Appendix A for a derivation of an alternative version of Theorem 6.1.

Finally, as a simple corollary of Theorem 6.1, we obtain the following representation for finitely exchangeable quantum states.

Corollary 6.2 (Finite Quantum de Finetti Representation). *Let $\mathcal{H}$ be a d-dimensional Hilbert space and let $\rho^{\overline{n}} \in \mathrm{S}(\mathcal{H}^{\otimes n})$ be $(n + s)$-exchangeable. Then $\rho^{\overline{n}}$ is ε-close to the convex hull of the set of n-fold product states $\{\sigma^{\otimes n} : \sigma \in \mathrm{S}(\mathcal{H})\}$, for $\varepsilon = \sqrt{2}\, \bar{C}_2(d)n/\sqrt{s}$.*

Proof. Let $k := \lceil s/2 \rceil$ and let $\rho^{\overline{n+k}} \in \mathrm{S}(\mathcal{H}^{\otimes n+k})$ be an $(n + 2k - 1)$-exchangeable extension of $\rho^{\overline{n}}$. Let $\mathfrak{Z}$ be an informationally complete POVM on $\mathcal{H}$ and let, for any $\bar{\mathbf{z}} \in \mathcal{Z}^k$, $\rho^{\overline{n}}_{\bar{\mathbf{z}}} := \rho^{\overline{n}}_{|\mathfrak{Z}^k = \bar{\mathbf{z}}}$. We show that

$$\delta(\rho^{\overline{n}}, \mathbb{E}_{\bar{\mathbf{z}}}\big[(\rho^{\overline{1}}_{\bar{\mathbf{z}}})^{\otimes n}\big]) \leq \sqrt{2}\, \bar{C}_2(d)\frac{n}{\sqrt{s}} \ . \tag{34}$$

where $\bar{\mathbf{z}} \leftarrow \rho^{\overline{k}}_{\mathfrak{Z}^k}$ Since, by (1),

$$\mathbb{E}_{\bar{\mathbf{z}}}\big[\rho^{\overline{n}}_{\bar{\mathbf{z}}}\big] = \rho^{\overline{n}} \ ,$$

we obtain, using the strong convexity of the trace distance

$$\delta(\rho^{\overline{n}}, \mathbb{E}_{\bar{\mathbf{z}}}\big[(\rho^{\overline{1}}_{\bar{\mathbf{z}}})^{\otimes n}\big]) = \delta(\mathbb{E}_{\bar{\mathbf{z}}}\big[\rho^{\overline{n}}_{\bar{\mathbf{z}}}\big], \mathbb{E}_{\bar{\mathbf{z}}}\big[(\rho^{\overline{1}}_{\bar{\mathbf{z}}})^{\otimes n}\big]) \leq \mathbb{E}_{\bar{\mathbf{z}}}[\delta(\rho^{\overline{n}}_{\bar{\mathbf{z}}}, (\rho^{\overline{1}}_{\bar{\mathbf{z}}})^{\otimes n})] \ . \tag{35}$$

Inequality (34) then follows directly from Theorem 6.1. $\square$

While this result is of interest in its on right, we point out that taking the limit $s \to \infty$ directly gives the well-known quantum de Finetti representation for *infinitely* exchangeable quantum states [HM76], thus providing yet another new (compare [CFS02]) and conceptually simple proof.

7 Acknowledgment

A   A Markov-style version of Theorem 6.1

While Theorem 6.1 provides a bound on the expected distance between the conditional state $\rho_{\bar{\mathbf{z}}}^{A\overline{n}}$ and the product state $\rho_{\bar{\mathbf{z}}}^A \otimes (\rho_{\bar{\mathbf{z}}}^{\overline{1}})^{\otimes n}$, Theorem A.1 below gives an expression for the minimum probability such that this distance is smaller than some given value.

Theorem A.1. *Let $\rho^{A\overline{n+k}} \in \mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}^{\otimes n+k})$ be $(n+2k-1)$-exchangeable relative to $\mathcal{H}_A$ and let $\mathfrak{Z} = \{F_z\}_{z \in \mathcal{Z}}$ be a POVM on $\mathcal{H}$ with $|\mathcal{Z}| = t$. For every $\bar{\mathbf{z}} \in \mathcal{Z}^k$, let $\rho_{\bar{\mathbf{z}}}^{A\overline{n}} := \rho^{A\overline{n}}{}_{|\mathfrak{Z}^k = \bar{\mathbf{z}}}$. Then, for all $\varepsilon \geq 0$, and for $\bar{\mathbf{z}} \leftarrow \rho_{\mathfrak{Z}^k}^{\overline{k}}$, with probability at least $1 - k e^{-\varepsilon^2/2 + 1}$,*

$$\delta\big(\rho_{\bar{\mathbf{z}}}^{A\overline{n}}, \rho_{\bar{\mathbf{z}}}^A \otimes (\rho_{\bar{\mathbf{z}}}^{\overline{1}})^{\otimes n}\big) < \frac{n}{\sqrt{k}} C_2(\mathfrak{Z})\, \varepsilon$$

and

$$\delta\big(\rho_{\mathfrak{Z}|\mathfrak{Z}^k = \bar{\mathbf{z}}}^{\overline{1}}, Q_{\bar{\mathbf{z}}}\big) < \sqrt{\frac{t}{k}}\varepsilon\ .$$

The proof of this theorem essentially follows the lines of the proof of Theorem 6.1. The main difference is that Lemma 4.2 is replaced by a statement based on a tail inequality due to Hoeffding [Hoe63] which applies to hypergeometric distributions as defined below (for more details, see, e.g., [JLR00]).

Definition A.2. *The* hypergeometric distribution *with parameters n, m, and k, denoted $\mathrm{Hyp}(n, m, k)$, is defined as the probability distribution of the random variable $S := |\Gamma \cap [m]|$ where Γ is a randomly chosen subset of $[n]$ of size $|\Gamma| = k$.*

Lemma A.3 (Hoeffding). *Let S be a random variable with $P_S = \mathrm{Hyp}(n, m, k)$. Then, for all $\ell \geq 0$,*

$$\mathbb{P}[S \leq k\frac{m}{n} - \ell] \leq e^{-\frac{\ell^2 n}{2km}}\ .$$

Lemma A.4 and Lemma A.5 are adapted versions of Lemma 4.2 and Lemma 4.3, as proven in Section 4.1 and Section 4.2, respectively.

Lemma A.4. *Let $\mathbf{Z}$ be an n-tuple and $\bar{\mathbf{Z}}$ a k-tuple of random variables over a set $\mathcal{Z}$ of size $|\mathcal{Z}| = t$ such that $P_{(\mathbf{Z}, \bar{\mathbf{Z}})}$ is symmetric. Then, for any $\varepsilon \geq 0$ and for $(\mathbf{z}, \bar{\mathbf{z}}) \leftarrow P_{(\mathbf{Z}, \bar{\mathbf{Z}})}$,*

$$\mathbb{P}_{(\mathbf{z}, \bar{\mathbf{z}})}\big[\delta(Q_{\bar{\mathbf{z}}}, Q_{(\bar{\mathbf{z}}, \mathbf{z})}) \geq \varepsilon\big] \leq t\, e^{-\frac{k\varepsilon^2}{2t}}\ .$$

Proof. It suffices to show that, for all probability distributions $q \in \mathrm{Distr}(\mathcal{Z})$,

$$\mathbb{P}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z}, \bar{\mathbf{Z}})} = q}}\big[\delta(Q_{\bar{\mathbf{z}}}, q) \geq \varepsilon\big] \leq t\, e^{-\frac{k\varepsilon^2}{2t}}\ . \tag{36}$$

The assertion of the lemma then follows from

$$\mathbb{P}_{(\mathbf{z}, \bar{\mathbf{z}}) \leftarrow P_{(\mathbf{Z}, \bar{\mathbf{Z}})}}\big[\delta(Q_{\bar{\mathbf{z}}}, Q_{(\mathbf{z}, \bar{\mathbf{z}})}) \geq \varepsilon\big] = \mathbb{E}_{q \leftarrow P_{Q_{(\mathbf{Z}, \bar{\mathbf{Z}})}}}\Big[\mathbb{P}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z}, \bar{\mathbf{Z}})} = q}}\big[\delta(Q_{\bar{\mathbf{z}}}, q) \geq \varepsilon\big]\Big]\ .$$

Let thus $q \in \mathrm{Distr}(\mathcal{Z})$ with $P_{Q_{(\mathbf{Z}, \bar{\mathbf{Z}})}}(q) > 0$ be fixed. The variational distance between $Q_{\bar{\mathbf{z}}}$ and q can be written as

$$\delta(Q_{\bar{\mathbf{z}}}, q) = \sum_{z \in \mathcal{Z}'} \max\big(q(z) - Q_{\bar{\mathbf{z}}}(z), 0\big)\ . \tag{37}$$

where $\mathcal{Z}' := \{z \in \mathcal{Z} : q(z) > 0\}$. It is easy to see that, for any $z \in \mathcal{Z}$, the random variable $S_z := k \cdot Q_{\bar{\mathbf{z}}}(z)$, conditioned on the event $Q_{(\mathbf{Z}, \bar{\mathbf{Z}})} = q$, is distributed according to $\mathrm{Hyp}(n + k, (n + k)\, q(z), k)$. For any $z \in \mathcal{Z}'$, let $\varepsilon_z := \varepsilon\sqrt{q(z)/t}$. Lemma A.3 (with $\ell = k\varepsilon_z$) then implies

$$\mathbb{P}_{\bar{\mathbf{z}} \leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z}, \bar{\mathbf{Z}})} = q}}\big[q(z) - Q_{\bar{\mathbf{z}}}(z) \geq \varepsilon_z\big] \leq e^{-\frac{k\varepsilon_z^2}{2q(z)}} = e^{-\frac{k\varepsilon^2}{2t}}\ ,$$

and thus, using the union bound,

$$\mathbb{P}_{\bar{\mathbf{z}}\leftarrow P_{\bar{\mathbf{Z}}|Q_{(\mathbf{Z},\bar{\mathbf{Z}})}=q}}\Big[\forall z\in\mathcal{Z}':q(z)-Q_{\bar{\mathbf{z}}}(z)<\varepsilon\sqrt{\frac{q(z)}{t}}\Big]\geq 1-t\,e^{-\frac{k\varepsilon^2}{2t}}\ . \tag{38}$$

Since, by Jensen's inequality,

$$\sum_{z\in\mathcal{Z}'}\varepsilon\sqrt{\frac{q(z)}{t}}\leq\varepsilon\sqrt{\sum_{z\in\mathcal{Z}'}q(z)}=\varepsilon$$

the event in (38) implies that the sum on the r.h.s. of (37) is smaller than ε, that is, $\delta(Q_{\bar{\mathbf{z}}},q)<\varepsilon$. Inequality (36) thus follows directly from the bound (38). $\qquad\square$

Lemma A.5. *Let $\mathbf{Z}$ be an n-tuple and $\bar{\mathbf{Z}}$ a k-tuple of random variables over a set $\mathcal{Z}$ of size $|\mathcal{Z}|=t$, for $k\leq n$, such that $P_{(\mathbf{Z},\bar{\mathbf{Z}})}$ is symmetric. Then, for all $\varepsilon\geq 0$ and for $\bar{\mathbf{z}}\leftarrow P_{\bar{\mathbf{Z}}}$,*

$$\mathbb{P}_{\bar{\mathbf{z}}}[D_{Q_{\bar{\mathbf{z}}}}(P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}})\geq\varepsilon]\leq k\,e^{-\frac{k\varepsilon^2}{2t}+1}\ .$$

Proof. Let $\tau:=\frac{t}{k}$ and $\bar{\varepsilon}:=\varepsilon-\tau$. Note that, if $\varepsilon\leq\tau$, the r.h.s. of the inequality in the lemma becomes larger than 1 because $\varepsilon\leq 1$, i.e., the assertion is trivially true. Thus we can assume that $\bar{\varepsilon}>0$. For all $\bar{\mathbf{z}}\in\mathcal{Z}^k$, let

$$p_{\bar{\mathbf{z}}}:=\mathbb{P}_{\mathbf{z}\leftarrow P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}}}[\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})\geq\bar{\varepsilon}]\ .$$

We then have, by Lemma A.4,

$$\mathbb{E}_{\bar{\mathbf{z}}\leftarrow P_{\bar{\mathbf{Z}}}}[p_{\bar{\mathbf{z}}}]=\mathbb{P}_{(\mathbf{z},\bar{\mathbf{z}})\leftarrow P_{(\mathbf{Z},\bar{\mathbf{Z}})}}[\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})\geq\bar{\varepsilon}]\leq t\,e^{-\frac{k\bar{\varepsilon}^2}{2t}}\ ,$$

and, by Markov's inequality,

$$\mathbb{P}_{\bar{\mathbf{z}}\leftarrow P_{\bar{\mathbf{Z}}}}[p_{\bar{\mathbf{z}}}\geq\tau]\leq\frac{t}{\tau}\,e^{-\frac{k\bar{\varepsilon}^2}{2t}}\ . \tag{39}$$

With the definition

$$\Lambda:=\{\bar{\mathbf{z}}\in\mathcal{Z}^k:p_{\bar{\mathbf{z}}}<\tau\}\ ,$$

the bound (39) can be rewritten as

$$\mathbb{P}_{\bar{\mathbf{z}}\leftarrow P_{\bar{\mathbf{Z}}}}[\bar{\mathbf{z}}\notin\Lambda]\leq\frac{t}{\tau}\,e^{-\frac{k\bar{\varepsilon}^2}{2t}}\leq k\,e^{-\frac{k\varepsilon^2}{2t}+1}$$

where the second inequality follows from the observation that $\bar{\varepsilon}^2=(\varepsilon-\tau)^2\geq\varepsilon^2-2\tau$ and $\tau=\frac{t}{k}$.

It thus remains to be shown that, for any $\bar{\mathbf{z}}\in\Lambda$,

$$D_{Q_{\bar{\mathbf{z}}}}(P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}})=\mathbb{E}_{\mathbf{z}\leftarrow P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}}}[\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})]<\varepsilon\ . \tag{40}$$

Let thus $\bar{\mathbf{z}}\in\Lambda$ be fixed. Then

$$\mathbb{E}_{\mathbf{z}\leftarrow P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}}}[\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})]=\sum_{\substack{\mathbf{z}\in\mathcal{Z}^n\\\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})<\bar{\varepsilon}}}P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}}(\mathbf{z})\,\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})\ +\sum_{\substack{\mathbf{z}\in\mathcal{Z}^n\\\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})\geq\bar{\varepsilon}}}P_{\mathbf{Z}|\bar{\mathbf{Z}}=\bar{\mathbf{z}}}(\mathbf{z})\,\delta(Q_{\mathbf{z}},Q_{\bar{\mathbf{z}}})<\bar{\varepsilon}+p_{\bar{\mathbf{z}}}$$

from which the bound (40) follows by the definition of Λ and $\bar{\varepsilon}+\tau=\varepsilon$. $\qquad\square$

Finally, using Lemma A.5, we directly obtain Lemma A.6 below which corresponds to Lemma 5.7 of Section 5.2.

Lemma A.6. *Let $\rho^{\overline{n+k}}\in\mathrm{S}(\mathcal{H}^{\otimes n+k})$, for $k\leq n$, be symmetric and let $\mathfrak{Z}=\{F_z\}_{z\in\mathcal{Z}}$ be a POVM on $\mathcal{H}$ with $|\mathcal{Z}|=t$. Then, for all $\varepsilon\geq 0$ and for $\bar{\mathbf{z}}\leftarrow\rho_{\mathfrak{Z}^k}^{\bar{k}}$,*

$$\mathbb{P}_{\bar{\mathbf{z}}}\big[D_{Q_{\bar{\mathbf{z}}}}(\rho_{\mathfrak{Z}^n|\mathfrak{Z}^k=\bar{\mathbf{z}}}^{\overline{n}})\geq\varepsilon\big]\leq k e^{-\frac{k\varepsilon^2}{2t}+1}\ .$$

The proof of Theorem A.1 is now similar to the proof of Theorem 6.1, where, instead of Lemma 5.7, Lemma A.6 is used to bound the r.h.s. of (32) and (33).

References

[BB84]   C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[CFS02]   C. M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: The quantum de Finetti representation. *J. Math. Phys.*, 43(4537), 2002. http://www.arxiv.org/abs/quant-ph/0104088.

[CRE04]   M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key distribution. http://arxiv.org/abs/quant-ph/0402131, February 2004.

[dF37]   B. de Finetti. La prévision: ses lois logiques, ses sources subjectives. *Ann. Inst. H. Poincaré*, 7:1–68, 1937.

[DF80]   P. Diaconis and D. Freedman. Finite exchangeable sequences. *The Annals of Probability*, 8(4):745–764, 1980.

[DPS04]   G. M. D'Ariano, P. Perinotti, and M. F. Sacchi. Informationally complete measurements and group representation. *J. Opt. B: Quantum and Semicl. Optics*, 6:487–491, 2004. http://arxiv.org/abs/quant-ph/0310013.

[Eke91]   A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[FS04]   C. A. Fuchs and R. Schack. Unknown quantum states and operations, a Bayesian view. http://www.arxiv.org/abs/quant-ph/0404156, 2004.

[Gra04]   M. Grassl. On SIC-POVMs and MUBs in dimension 6. http://arxiv.org/abs/quant-ph/0406175, 2004.

[HM76]   R. L. Hudson and G. R. Moody. Locally normal symmetric states and an analogue of de Finetti's theorem. *Z. Wahrschein. verw. Geb.*, 33:343–351, 1976.

[Hoe63]   W. Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, March 1963.

[Hud81]   R. L. Hudson. Analogs of de Finetti's theorem and interpretative problems of quantum mechanics. *Found. Phys.*, 11:805–808, 1981.

[JLR00]   S. Janson, T. Luczak, and A. Rucinski. *Random Graphs*. Wiley, 2000.

[MC93]   P. Monari and D. Cocchi, editors. *Introduction to Bruno de Finetti's "Probabiliá e Induzione"*. Cooperativa Libraria Universitaria Editrice, Bologna, 1993.

[RBKSC04] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45(2171), 2004. http://arxiv.org/abs/quant-ph/0310075.