CS 766/QIC 820 Theory of Quantum Information (Fall 2011)

# Lecture 22: The finite quantum de Finetti theorem

The main goal of this lecture is to prove a theorem known as the *quantum de Finetti theorem*. There are, in fact, multiple variants of this theorem, so to be more precise it may be said that we will prove a theorem of the quantum de Finetti type. This type of theorem states, in effect, that if a collection of identical quantum registers have a state that is invariant under permutations, then the reduced state of a comparatively small number of these registers must be close to a convex combination of identical product states.

There will be three main parts of this lecture. First, we will introduce various concepts concerning quantum states of multiple register systems that are invariant under permutations of these registers. We will then very briefly discuss integrals defined with respect to the unitarily invariant measure on the unit sphere of a given complex Euclidean space, which will supply us with a useful tool we need for the last part of the lecture. The last part of the lecture is the statement and proof of the quantum de Finetti theorem.

It is inevitable that some details regarding integrals over unitarily invariant measure will be absent from the lecture (and from these notes). The main reason for this is that we have very limited time remaining in the course, and certainly not enough time for a proper discussion of the details. Also, the background knowledge needed to formalize the details is rather different from what was required for other lectures. Nevertheless, I hope there will be enough information for you to follow up on this lecture on your own, in case you choose to do this.

## 22.1 Symmetric subspaces and exchangeable operators

Let us fix a finite, nonempty set $\Sigma$, and let $d = |\Sigma|$ for the remainder of this lecture. Also let $n$ be a positive integer, and let $\mathsf{X}_1, \ldots, \mathsf{X}_n$ be identical quantum registers, with associated complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ taking the form $\mathcal{X}_k = \mathbb{C}^\Sigma$ for $1 \leq k \leq n$.

### 22.1.1 Permutation operators

For each permutation $\pi \in S_n$, we define a unitary operator

$$W_\pi \in \mathrm{U}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right)$$

by the action

$$W_\pi(u_1 \otimes \cdots \otimes u_n) = u_{\pi^{-1}(1)} \otimes \cdots \otimes u_{\pi^{-1}(n)}$$

for every choice of vectors $u_1, \ldots, u_n \in \mathbb{C}^\Sigma$. In other words, $W_\pi$ permutes the contents of the registers $\mathsf{X}_1, \ldots, \mathsf{X}_n$ according to $\pi$. It holds that

$$W_\pi W_\sigma = W_{\pi\sigma} \qquad \text{and} \qquad W_\pi^{-1} = W_\pi^* = W_{\pi^{-1}} \tag{22.1}$$

for all $\pi, \sigma \in S_n$.

### 22.1.2 The symmetric subspace

Some vectors in $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ are invariant under the action of $W_\pi$ for every choice of $\pi \in S_n$, and it holds that the set of all such vectors forms a subspace. This subspace is called the *symmetric subspace*, and will be denoted in these notes as $\mathcal{X}_1 \ovee \cdots \ovee \mathcal{X}_n$. In more precise terms, this subspace is defined as

$$\mathcal{X}_1 \ovee \cdots \ovee \mathcal{X}_n = \{u \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n \,:\, u = W_\pi u \text{ for every } \pi \in S_n\}\,.$$

One may verify that the orthogonal projection operator that projects onto this subspace is given by

$$\Pi_{\mathcal{X}_1 \ovee \cdots \ovee \mathcal{X}_n} = \frac{1}{n!} \sum_{\pi \in S_n} W_\pi.$$

Let us now construct an orthonormal basis for the symmetric subspace. First, consider the set $\operatorname{Urn}(n, \Sigma)$ of functions of the form $\phi : \Sigma \to \mathbb{N}$ (where $\mathbb{N} = \{0, 1, 2, \ldots\}$) that satisfy

$$\sum_{a \in \Sigma} \phi(a) = n.$$

The elements of this set describe *urns* containing $n$ marbles, where each marble is labelled by an element of $\Sigma$. (There is no order associated with the marbles—all that matters is how many marbles with each possible label are contained in the urn. Urns are also sometimes called *bags*, and may alternately be described as multisets of elements of $\Sigma$ having $n$ items in total.)

Now, to say that a string $a_1 \cdots a_n \in \Sigma$ is *consistent* with a particular function $\phi \in \operatorname{Urn}(n, \Sigma)$ means simply that $a_1 \cdots a_n$ is one possible ordering of the marbles in the urn described by $\phi$. One can express this formally by defining a function

$$f_{a_1 \cdots a_n}(b) = \left|\{j \in \{1, \ldots, n\} \,:\, b = a_j\}\right|,$$

and by defining that $a_1 \cdots a_n$ is consistent with $\phi$ if and only if $f_{a_1 \cdots a_n} = \phi$. The number of distinct strings $a_1 \cdots a_n \in \Sigma^n$ that are consistent with a given function $\phi \in \operatorname{Urn}(n, \Sigma)$ is given by the multinomial coefficient

$$\binom{n}{\phi} \triangleq \frac{n!}{\prod_{a \in \Sigma} (\phi(a)!)}.$$

Finally, we define an orthonormal basis of $\mathcal{X}_1 \ovee \cdots \ovee \mathcal{X}_n$ as $\{u_\phi \,:\, \phi \in \operatorname{Urn}(n, \Sigma)\}$, where

$$u_\phi = \binom{n}{\phi}^{-1/2} \sum_{\substack{a_1 \cdots a_n \in \Sigma^n \\ f_{a_1 \cdots a_n} = \phi}} e_{a_1} \otimes \cdots \otimes e_{a_n}.$$

In other words, $u_\phi$ is the uniform pure state over all of the strings that are consistent with the function $\phi$.

For example, taking $n = 3$ and $\Sigma = \{0, 1\}$, we obtain the following four vectors:

$$\begin{aligned}
u_0 &= e_0 \otimes e_0 \otimes e_0 \\
u_1 &= \frac{1}{\sqrt{3}} (e_0 \otimes e_0 \otimes e_1 + e_0 \otimes e_1 \otimes e_0 + e_1 \otimes e_0 \otimes e_0) \\
u_2 &= \frac{1}{\sqrt{3}} (e_0 \otimes e_1 \otimes e_1 + e_1 \otimes e_0 \otimes e_1 + e_1 \otimes e_1 \otimes e_0) \\
u_3 &= e_1 \otimes e_1 \otimes e_1,
\end{aligned}$$

where the vectors are indexed by integers rather than functions $\phi \in \mathrm{Urn}(3, \{0,1\})$ in a straightforward way.

Using simple combinatorics, it can be shown that $|\mathrm{Urn}(n,\Sigma)| = \binom{n+d-1}{d-1}$, and therefore

$$\dim(\mathcal{X}_1 \varovee \cdots \varovee \mathcal{X}_n) = \binom{n+d-1}{d-1}.$$

Notice that for small $d$ and large $n$, the dimension of the symmetric subspace is therefore very small compared with the entire space $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$.

It is also the case that

$$\mathcal{X}_1 \varovee \cdots \varovee \mathcal{X}_n = \operatorname{span}\left\{ u^{\otimes n} \,:\, u \in \mathbb{C}^{\Sigma} \right\}.$$

This follows from an elementary fact concerning the theory of symmetric functions, but I will not prove it here.

### 22.1.3 Exchangeable operators and their relation to the symmetric subspace

Along similar lines to vectors in the symmetric subspace, we say that a positive semidefinite operator $P \in \mathrm{Pos}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right)$ is *exchangeable* if it is the case that

$$P = W_\pi P W_\pi^*$$

for every $\pi \in S_n$.

It is the case that every positive semidefinite operator whose image is contained in the symmetric subspace is exchangeable, but this is not a necessary condition. For instance, the identity operator $\mathbb{1}_{\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n}$ is exchangeable and its image is all of $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$. We may, however, relate exchangeable operators and the symmetric subspace by means of the following lemma.

**Lemma 22.1.** *Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be copies of the complex Euclidean space $\mathbb{C}^{\Sigma}$, and suppose that*

$$P \in \mathrm{Pos}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right)$$

*is an exchangeable operator. There exists a symmetric vector*

$$u \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \varovee \cdots \varovee (\mathcal{X}_n \otimes \mathcal{Y}_n)$$

*that purifies $P$, i.e., $\mathrm{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(uu^*) = P$.*

*Proof.* Consider a spectral decomposition

$$P = \sum_{j=1}^{k} \lambda_j Q_j, \tag{22.2}$$

where $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of $P$ and $Q_1, \ldots, Q_k$ are orthogonal projection operators onto the associated eigenspaces. As $W_\pi P W_\pi^* = P$ for each permutation $\pi \in S_n$, it follows that $W_\pi Q_j W_\pi^* = Q_j$ for each $j = 1, \ldots, k$, owing to the fact that the decomposition (22.2) is unique. The operator $\sqrt{P}$ is therefore also exchangeable, so that

$$(W_\pi \otimes W_\pi) \operatorname{vec}\left(\sqrt{P}\right) = \operatorname{vec}\left(W_\pi \sqrt{P} W_\pi^{\mathsf{T}}\right) = \operatorname{vec}\left(W_\pi \sqrt{P} W_\pi^*\right) = \operatorname{vec}\left(\sqrt{P}\right).$$

Now let us view the operator $\sqrt{P}$ as taking the form

$$\sqrt{P} \in \mathrm{L}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n\right)$$

by identifying $\mathcal{Y}_j$ with $\mathcal{X}_j$ for $j = 1, \ldots, n$. We therefore have

$$\operatorname{vec}\left(\sqrt{P}\right) \in \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n \otimes \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n.$$

Let us take $u \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes \cdots \otimes (\mathcal{X}_n \otimes \mathcal{Y}_n)$ to be equal to this vector, but with the tensor factors re-ordered in a way that is consistent with the names of the associated spaces. It holds that $\operatorname{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(uu^*) = P$, and given that

$$(W_\pi \otimes W_\pi) \operatorname{vec}\left(\sqrt{P}\right) = \operatorname{vec}\left(\sqrt{P}\right)$$

for all $\pi \in S_n$ it follows that $u \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \varovee \cdots \varovee (\mathcal{X}_n \otimes \mathcal{Y}_n)$ as required. □

## 22.2 Integrals and unitarily invariant measure

For the proof of the main result in the next section, we will need to be able to express certain linear operators as integrals. Here is a very simple expression that will serve as an example for the sake of this discussion:

$$\int uu^* \, \mathrm{d}\mu(u).$$

Now, there are two very different questions one may have about such an operator:

1. What does it mean in formal terms?
2. How is it calculated?

The answer to the first question is a bit complicated—and although we will not have time to discuss it in detail, I would like to say enough to at least give you some clues and key-words in case you wish to learn more on your own.

In the above expression, $\mu$ refers to the normalized *unitarily invariant measure* defined on the Borel sets of the unit sphere $\mathcal{S} = \mathcal{S}(\mathcal{X})$ in some chosen complex Euclidean space $\mathcal{X}$. (The space $\mathcal{X}$ is implicit in the above expression, and generally would be determined by the context of the expression.) To say that $\mu$ is *normalized* means that $\mu(\mathcal{S}) = 1$, and to say that $\mu$ is *unitarily invariant* means that $\mu(\mathcal{A}) = \mu(U(\mathcal{A}))$ for every Borel set $\mathcal{A} \subseteq \mathcal{S}$ and every unitary operator $U \in \mathrm{U}(\mathcal{X})$. It turns out that there is only one measure with the properties that have just been described. Sometimes this measure is called *Haar measure*, although this term is considerably more general than what we have just described. (There is a uniquely defined Haar measure on many different sorts of measure spaces with groups acting on them in a particular way.)

Informally speaking, you may think of the measure described above as a way of assigning an infinitesimally small probability to each point on the unit sphere in such a way that no one vector is weighted more or less than any other. So, in an integral like the one above, we may view that it is an average of operators $uu^*$ over the entire unit sphere, with each $u$ being given equal weight. Of course it does not really work this way, which is why we must speak of Borel sets rather than arbitrary sets—but it is a reasonable guide for the simple uses of it in this lecture.

In formal terms, there is a process involving several steps for building up the meaning of an integral like the one above starting from the measure $\mu$. It starts with characteristic functions for

Borel sets (where the value of the integral is simply the set's measure), then it defines integrals for positive linear combinations of characteristic functions in the obvious way, then it introduces limits to define integrals of more functions, and continues for a few more steps until we finally have integrals of operators. Needless to say, this process does not provide an efficient means to calculate a given integral.

This leads us to the second question, which is how to calculate such integrals. There is certainly no general method: just like ordinary integrals you are lucky when there is a closed form. For some, however, the fact that the measure is unitarily invariant leads to a simple answer. For instance, the integral above must satisfy

$$\int uu^* \,\mathrm{d}\mu(u) = U\left(\int uu^* \,\mathrm{d}\mu(u)\right)U^*$$

for every unitary operator $U \in \mathrm{U}(\mathcal{X})$, and must also satisfy

$$\operatorname{Tr}\left(\int uu^* \,\mathrm{d}\mu(u)\right) = \int \mathrm{d}\mu(u) = \mu(\mathcal{S}) = 1.$$

There is only one possibility:

$$\int uu^* \,\mathrm{d}\mu(u) = \frac{1}{\dim(\mathcal{X})}\mathbb{1}_{\mathcal{X}}.$$

Now, what we need for the next part of the lecture is a generalization of this fact—which is that for every $n \geq 1$ we have

$$\binom{n+d-1}{d-1}\int (uu^*)^{\otimes n} \,\mathrm{d}\mu(u) = \Pi_{\mathcal{X}_1 \varovee \cdots \varovee \mathcal{X}_n}\,,$$

the projection onto the symmetric subspace. This is yet another fact for which a complete proof would be too much of a diversion at this point in the course. The main result we need is a fact from algebra that states that every operator in the space $\mathrm{L}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$ that commutes with $U^{\otimes n}$ for every unitary operator $U \in \mathrm{U}(\mathbb{C}^\Sigma)$ must be a linear combination of the operators $\{W_\pi : \pi \in S_n\}$. Given this fact, along with the fact that the operator expressed by the integral has the correct trace and is invariant under multiplication by every $W_\pi$, the proof follows easily.

## 22.3 The quantum de Finetti theorem

Now we are ready to state and prove (one variant of) the quantum de Finetti theorem, which is the main goal of this lecture. The statement and proof follow.

**Theorem 22.2.** *Let $\mathsf{X}_1, \ldots, \mathsf{X}_n$ be identical quantum registers, each having associated space $\mathbb{C}^\Sigma$ for $|\Sigma| = d$, and let $\rho \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$ be an exchangeable density operator representing the state of these registers. For any choice of $k \in \{1, \ldots, n\}$, there exists a finite set $\Gamma$, a probability vector $p \in \mathbb{R}^\Gamma$, and a collection of density operators $\{\xi_a : a \in \Gamma\} \subset \mathrm{D}(\mathbb{C}^\Sigma)$ such that*

$$\left\| \rho^{\mathsf{X}_1\cdots\mathsf{X}_k} - \sum_{a\in\Gamma} p(a)\xi_a^{\otimes k} \right\|_1 < \frac{4d^2k}{n}.$$

*Proof.* First we will prove a stronger bound for the case where $\rho = vv^*$ is pure (which requires $v \in \mathcal{X}_1 \circledvee \cdots \circledvee \mathcal{X}_n$). This will then be combined with Lemma 22.1 to complete the proof.

For the sake of clarity, let us write $\mathcal{Y} = \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$ and $\mathcal{Z} = \mathcal{X}_{k+1} \otimes \cdots \otimes \mathcal{X}_n$. Let us also write

$$S^{(m)} = \binom{m+d-1}{d-1} \int (uu^*)^{\otimes m} \, \mathrm{d}\mu(u),$$

which is the projection onto the symmetric subspace of $m$ copies of $\mathbb{C}^\Sigma$ for any choice of $m \geq 1$.

Now consider a unit vector $v \in \mathcal{X}_1 \circledvee \cdots \circledvee \mathcal{X}_n$. As $v$ is invariant under every permutation of its tensor factors, it holds that

$$v = \left(\mathbb{1}_{\mathcal{Y}} \otimes S^{(n-k)}\right) v.$$

Therefore, for $\sigma \in \mathrm{D}(\mathcal{Y})$ defined as $\sigma = \operatorname{Tr}_{\mathcal{Z}}(vv^*)$ we must have

$$\sigma = \operatorname{Tr}_{\mathcal{Z}} \left( \left(\mathbb{1}_{\mathcal{Y}} \otimes S^{(n-k)}\right) vv^* \right).$$

Defining a mapping $\Phi_u \in \mathrm{T}(\mathcal{Y} \otimes \mathcal{Z}, \mathcal{Y})$ for each vector $u \in \mathbb{C}^\Sigma$ as

$$\Phi_u(X) = \left(\mathbb{1}_{\mathcal{Y}} \otimes u^{\otimes(n-k)}\right)^* X \left(\mathbb{1}_{\mathcal{Y}} \otimes u^{\otimes(n-k)}\right)$$

for every $X \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{Z})$, we have

$$\sigma = \binom{n-k+d-1}{d-1} \int \Phi_u(vv^*) \, \mathrm{d}\mu(u).$$

Now, our goal is to approximate $\sigma$ by a density operator taking the form

$$\sum_{a \in \Gamma} p(a) \xi_a^{\otimes k},$$

so we will guess a suitable approximation:

$$\tau = \binom{n+d-1}{d-1} \int \left\langle (uu^*)^{\otimes k}, \Phi_u(vv^*) \right\rangle (uu^*)^{\otimes k} \, \mathrm{d}\mu(u).$$

It holds that $\tau$ has trace 1, because

$$\operatorname{Tr}(\tau) = \binom{n+d-1}{d-1} \int \left\langle (uu^*)^{\otimes n}, vv^* \right\rangle \mathrm{d}\mu(u) = \left\langle S^{(n)}, vv^* \right\rangle = 1,$$

and $\tau$ also has the correct form:

$$\tau \in \operatorname{conv} \left\{ (ww^*)^{\otimes k} \, : \, w \in \mathcal{S}\left(\mathbb{C}^\Sigma\right) \right\}.$$

(It is intuitive that this should be so, but we have not proved it formally. Of course it can be proved formally, but it requires details about measure and integration beyond what we have discussed.)

We will now place an upper bound on $\|\sigma - \tau\|_1$. To make the proof more readable, let us write

$$c_m = \binom{m+d-1}{d-1}$$

for each $m \geq 0$. We begin by noting that

$$\|\sigma - \tau\|_1 \leq \left\| \sigma - \frac{c_{n-k}}{c_n}\tau \right\|_1 + \left\| \frac{c_{n-k}}{c_n}\tau - \tau \right\|_1 = c_{n-k} \left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 + \left(1 - \frac{c_{n-k}}{c_n}\right). \tag{22.3}$$

Next, by making use of the operator equality

$$A - BAB = A(\mathbb{1} - B) + (\mathbb{1} - B)A - (\mathbb{1} - B)A(\mathbb{1} - B),$$

and writing $\Delta_u = (uu^*)^{\otimes k}$, we obtain

$$\begin{aligned}
\left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 &= \left\| \int \left(\Phi_u(vv^*) - \Delta_u \Phi_u(vv^*)\Delta_u\right) \mathrm{d}\mu(u) \right\|_1 \\
&\leq \left\| \int \Phi_u(vv^*)(\mathbb{1} - \Delta_u) \,\mathrm{d}\mu(u) \right\|_1 + \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*) \,\mathrm{d}\mu(u) \right\|_1 \\
&\quad + \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)(\mathbb{1} - \Delta_u) \,\mathrm{d}\mu(u) \right\|_1.
\end{aligned}$$

It holds that

$$\left\| \int \Phi_u(vv^*)(\mathbb{1} - \Delta_u) \,\mathrm{d}\mu(u) \right\|_1 = \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*) \,\mathrm{d}\mu(u) \right\|_1,$$

while

$$\begin{aligned}
\left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)(\mathbb{1} - \Delta_u) \,\mathrm{d}\mu(u) \right\|_1 &= \operatorname{Tr}\left( \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)(\mathbb{1} - \Delta_u) \,\mathrm{d}\mu(u) \right) \\
&= \operatorname{Tr}\left( \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*) \,\mathrm{d}\mu(u) \right) \\
&\leq \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*) \,\mathrm{d}\mu(u) \right\|_1.
\end{aligned}$$

Therefore we have

$$\left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 \leq 3 \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*) \,\mathrm{d}\mu(u) \right\|_1.$$

At this point we note that

$$\int \Phi_u(vv^*) \,\mathrm{d}\mu(u) = \frac{1}{c_{n-k}}\sigma$$

while

$$\int \Delta_u \Phi_u(vv^*) \,\mathrm{d}\mu(u) = \operatorname{Tr}_{\mathcal{Z}} \int (uu^*)^{\otimes n} vv^* \,\mathrm{d}\mu(u) = \frac{1}{c_n}\sigma.$$

Therefore we have

$$\left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 \leq 3 \left( \frac{1}{c_{n-k}} - \frac{1}{c_n} \right),$$

and so

$$\|\sigma - \tau\|_1 \leq 3\, c_{n-k} \left( \frac{1}{c_{n-k}} - \frac{1}{c_n} \right) + \left(1 - \frac{c_{n-k}}{c_n}\right) = 4 \left(1 - \frac{c_{n-k}}{c_n}\right).$$

To finish off the upper bound, we observe that

$$\frac{c_{n-k}}{c_n} = \frac{(n-k+d-1)(n-k+d-2)\cdots(n-k+1)}{(n+d-1)(n+d-2)\cdots(n+1)} \geq \left(\frac{n-k+1}{n+1}\right)^{d-1} > 1 - \frac{dk}{n},$$

and so

$$\|\sigma - \tau\|_1 < \frac{4dk}{n}.$$

This establishes essentially the bound given in the statement of the theorem, albeit only for pure states, but with $d^2$ replaced by $d$.

To prove the bound in the statement of the theorem for an arbitrary exchangeable density operator $\rho \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$, we first apply Lemma 22.1 to obtain a symmetric purification

$$v \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \varovee \cdots \varovee (\mathcal{X}_n \otimes \mathcal{Y}_n)$$

of $\rho$, where $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ represent isomorphic copies of $\mathcal{X}_1, \ldots, \mathcal{X}_n$. By the argument above, we have

$$\|\sigma - \tau\|_1 < \frac{4d^2k}{n},$$

where $\sigma = \mathrm{Tr}_{\mathcal{Z}}(vv^*)$ for $\mathcal{Z} = (\mathcal{X}_{k+1} \otimes \mathcal{Y}_{k+1}) \otimes \cdots \otimes (\mathcal{X}_n \otimes \mathcal{Y}_n)$ and where

$$\tau \in \operatorname{conv}\left\{(uu^*)^{\otimes k} \,:\, u \in \mathcal{S}\left(\mathbb{C}^{\Sigma} \otimes \mathbb{C}^{\Sigma}\right)\right\}.$$

Taking the partial trace over $\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k$ then gives the result. □