Quantum information theory (MAT4430) **Spring 2021**

Lecture 16: Werner states, twirling and the no-cloning theorem

Lecturer: Alexander Müller-Hermes

Last lecture, we have studied the actions of the permutation group and the unitary group on the space $\mathcal{H}^{\otimes N}$. In this lecture, we will see two applications of these ideas. We will first study a class of symmetric quantum states, which palys an important role in entanglement theory, and second, we will prove the so-called no-cloning theorem showing that it is impossible to copy quantum information.

1 Werner states

We will now apply the ideas of this lecture to define a family of symmetric quantum states.

Definition 1.1 (Werner states)**.** *A quantum state $\rho \in D\left(\mathbb{C}^d \otimes \mathbb{C}^d\right)$ is called a* Werner state *if $(U \otimes U)\rho = \rho(U \otimes U)$ for every $U \in \mathcal{U}\left(\mathbb{C}^d\right)$.*

What makes Werner states so nice, is that general quantum states can be mapped to this family by a natural symmetrization operation, which is called a *twirl.* This twirling operation can be even be performed in practice, and it is the first step of many protocols in quantum information theory to symmetrize the input in this way. Let us start with the following general statement about symmetrizing operations:

Theorem 1.2 (Twirling)**.** *The UU-twirl $T_{UU} : B(\mathbb{C}^d \otimes \mathbb{C}^d) \rightarrow B(\mathbb{C}^d \otimes \mathbb{C}^d)$ given by*

$$T_{UU}\left(X\right) = \int_{\mathcal{U}(\mathbb{C}^d)} \left(U \otimes U\right) X \left(U \otimes U\right)^{\dagger} d\eta(U),$$

is a selfadjoint quantum channel and we have

$$T_{UU}(X) = \langle P_{sym}, X\rangle_{HS} \frac{P_{sym}}{\text{Tr}\left[P_{sym}\right]} + \langle P_{asym}, X\rangle_{HS} \frac{P_{asym}}{\text{Tr}\left(P_{asym}\right)},$$

where

$$P_{sym} = \frac{1}{2}\left(\mathbb{1}_d \otimes \mathbb{1}_d + \mathbb{F}_d\right) \quad \text{and} \quad P_{asym} = \frac{1}{2}\left(\mathbb{1}_d \otimes \mathbb{1}_d - \mathbb{F}_d\right),$$

denote the projections onto the symmetric and the antisymmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$, respectively. Furthermore, note that

$$\text{Tr}\left[P_{sym}\right] = \frac{1}{2} d\left(d+1\right) \quad \text{and} \quad \text{Tr}\left[P_{asym}\right] = \frac{1}{2} d\left(d-1\right),$$

are the dimensions of these spaces.

Proof. Consider an operator $X \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$ and note that

$$(V \otimes V) T_{UU}\left(X\right) \left(V \otimes V\right)^{\dagger} = T_{UU}\left(X\right),$$

for every $V \in \mathcal{U}\left(\mathbb{C}^d\right)$ by unitary invariance of the Haar measure. Clearly, this equation shows that $\left[V \otimes V, T_{UU}\left(X\right)\right] = 0$ for each $V \in \mathcal{U}\left(\mathbb{C}^d\right)$ and by Theorem **??** we have

$$T_{UU}\left(X\right) = a \frac{P_{sym}}{\text{Tr}\left[P_{sym}\right]} + b \frac{P_{asym}}{\text{Tr}\left[P_{asym}\right]},$$

since

$$\mathrm{span}\{\mathbb{1}_d \otimes \mathbb{1}_d, \mathbb{F}_d\} = \mathrm{span}\{P_{sym}, P_{asym}\}.$$

Moreover, note that

$$(U \otimes \overline{U}) P_{sym} (U \otimes \overline{U})^\dagger = P_{sym},$$

and

$$(U \otimes \overline{U}) P_{asym} (U \otimes \overline{U})^\dagger = P_{asym},$$

such that

$$a = \langle P_{sym}, T_{UU}(X) \rangle_{HS} = \langle T_{UU}(P_{sym}), X \rangle_{HS} = \langle P_{sym}, X \rangle_{HS},$$

and

$$b = \langle P_{asym}, T_{UU}(X) \rangle_{HS} = \langle T_{UU}(P_{asym}), X \rangle_{HS} = \langle P_{asym}, X \rangle_{HS}.$$

This proves the formula for T_{UU} stated in the theorem. From this formula it is clear that T_{UU} is a selfadjoint quantum channel since the projectors P_{sym} and P_{asym} are positive semidefinite. □

Note that the Werner states are invariant under twirling, i.e., we have

$$T_{UU}(\rho) = \rho,$$

for any Werner state $\rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$. Since any quantum state ρ satisfies

$$1 = \mathrm{Tr}[\rho] = \langle P_{sym}, \rho \rangle_{HS} + \langle P_{asym}, \rho \rangle_{HS},$$

and

$$\langle P_{sym}, \rho \rangle_{HS} \geq 0 \quad \text{and} \quad \langle P_{asym}, \rho \rangle_{HS} \geq 0,$$

we have the the following corollary:

Corollary 1.3. *The Werner states on $\mathbb{C}^d \otimes \mathbb{C}^d$ are given by*

$$\rho_W(t) = (1-t)\frac{P_{sym}}{\mathrm{Tr}[P_{sym}]} + t\frac{P_{asym}}{\mathrm{Tr}(P_{asym})},$$

with $t \in [0,1]$. For any quantum state $\sigma \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$ we have

$$T_{UU}(\sigma) = \rho_W(t),$$

for $t = \langle P_{asym}, \sigma \rangle_{HS}$.

Finally, we will demonstrate how useful the symmetry of the Werner states is, by determining the parameter region in which they are entangled.

Theorem 1.4. *The following are equivalent:*

1. *The Werner state $\rho_W(t)$ is separable.*
2. *The Werner state $\rho_W(t)$ has positive partial transpose.*
3. *We have $t \leq 1/2$.*

Proof. Clearly, the first statement implies the second, and by direct computation it can be verified that the second statement implies the third. To see how the third statement implies the first, we will exploit the twirling operation. We start by noting that

$$\langle P_{sym}, |\phi\rangle\langle\phi| \otimes |\phi^\perp\rangle\langle\phi^\perp| \rangle_{HS} = \frac{1}{2} = \langle P_{asym}, |\phi\rangle\langle\phi| \otimes |\phi^\perp\rangle\langle\phi^\perp| \rangle_{HS},$$

for any pair of orthogonal pure states $|\phi\rangle, |\phi^{\perp}\rangle \in \mathbb{C}^d$. We can also check that

$$\langle P_{sym}, |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi|\rangle_{HS} = 1,$$

and

$$\langle P_{asym}, |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi|\rangle_{HS} = 0.$$

Using the formula of the UU-twirl we find that

$$\rho_W(t) = T_{UU}\left(|\phi\rangle\langle\phi| \otimes \left(2t|\phi\rangle\langle\phi| + (1-2t)|\phi^{\perp}\rangle\langle\phi^{\perp}|\right)\right),$$

whenever $0 \leq t \leq \frac{1}{2}$. But for any such t we then have

$$\rho_W(t) = \int_{u\in\mathcal{U}(\mathbb{C}^d)} U|\phi\rangle\langle\phi|U^{\dagger} \otimes \left(2tU|\phi\rangle\langle\phi|U^{\dagger} + (1-2t)U|\phi^{\perp}\rangle\langle\phi^{\perp}|U^{\dagger}\right) d\eta(U) \in \text{Sep}\left(\mathbb{C}^d, \mathbb{C}^d\right),$$

and the proof is finished. □

2 Impossibility of cloning and applications

2.1 The qualitative no-cloning theorem

The term "no-cloning theorem" is commonly used for the fact that unknown quantum states cannot be cloned or copied. The most common argument derives a contradiction from assuming a closed system with state space $\mathcal{H}$ undergoing some process modelled by a unitary $U \in \mathcal{U}(\mathcal{H})$ satisfying

$$U\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle, \tag{1}$$

for all pure states $|\psi\rangle \in \mathcal{H}$. Indeed such a unitary cannot exist, since otherwise

$$|\langle\psi|\phi\rangle|^2 = \left(\langle\psi| \otimes \langle 0|\right) U^{\dagger}U\left(|\phi\rangle \otimes |0\rangle\right) = |\langle\psi|\phi\rangle|,$$

for any pair of pure states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. However, this equation can only be satisfied if $|\langle\psi|\phi\rangle| = 0$ or $|\langle\psi|\phi\rangle| = 1$ leading to a contradiction since there are pure states satisfying neither. Note that this argument actually implies a stronger statement: No unitary $U \in \mathcal{U}(\mathcal{H})$ can satisfy (1) for distinct, non-orthogonal pure states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$. The assumption of non-orthogonality is crucial here and there are unitaries, e.g., the controlled-not gate, satisfying (1) for certain orthogonal pure states.

The previous argument might not seem fully general, since there could exist more general schemes for copying quantum information. The most general such operation would be some quantum channel $T : B(\mathcal{H}) \rightarrow B(\mathcal{H} \otimes \mathcal{H})$ satisfying

$$\left(\text{Tr} \otimes \text{id}_{B(\mathcal{H})}\right) \circ T = \left(\text{id}_{B(\mathcal{H})} \otimes \text{Tr}\right) \circ T = \text{id}_{B(\mathcal{H})}. \tag{2}$$

To show that such an operation does not exist, we recall that any quantum state $\rho_{AB} \in D\left(\mathcal{H} \otimes \mathcal{H}\right)$ satisfying $\rho_A = |\psi\rangle\langle\psi|$ and $\rho_B = |\psi\rangle\langle\psi|$ for some pure state $|\psi\rangle \in \mathcal{H}$ is necessarily of the form $\rho_{AB} = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|$. Therefore, (2) implies that

$$T\left(|\psi\rangle\langle\psi|\right) = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|,$$

for every pure state $|\psi\rangle\langle\psi| \in \text{Proj}\left(\mathcal{H}\right)$. We will now show that this property contradicts linearity of T. Write some pure state $|\psi\rangle\langle\psi| \in \text{Proj}\left(\mathcal{H}\right)$ as

$$|\psi\rangle\langle\psi| = \sum_{i=1}^{\dim(\mathcal{H})^2} \lambda_i |\psi_i\rangle\langle\psi_i|,$$

for $\{\lambda_i\}_i \subset \mathbb{R}$ and using a set of pure states $\{|\psi_i\rangle\langle\psi_i|\}_i$ which are linearly independent in $B(\mathcal{H})$. Then, we note that

$$\begin{aligned} T(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| &= \sum_{i,j} \lambda_i\lambda_j |\psi_i\rangle\langle\psi_i| \otimes |\psi_j\rangle\langle\psi_j| \\ &\neq \sum_{i=1}^{\dim(\mathcal{H})^2} \lambda_i |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{\dim(\mathcal{H})^2} \lambda_i T(|\psi_i\rangle\langle\psi_i|). \end{aligned}$$

We conclude that no quantum channel can satisfy (2) for every pure state $|\psi\rangle\langle\psi| \in \mathrm{Proj}(\mathcal{H})$ as quantum channels are always linear.

2.2 The quantitative no-cloning theorem

The previous argument shows that there is no quantum process that "clones" arbitrary pure states, i.e., implementing the map $|\phi\rangle \mapsto |\phi\rangle \otimes |\phi\rangle$. What about the map $|\phi\rangle^{\otimes n} \mapsto |\phi\rangle^{\otimes m}$ for $m > n$? We will now show that it is also impossible to find a quantum channel performing this task. Moreover, we will quantify how well a quantum channel can approximately succeed in it.

Theorem 2.1 (The quantitative no-cloning theorem)**.** *For any positive and trace-preserving linear map $T : B(\mathcal{H}^{\otimes n}) \to B(\mathcal{H}^{\otimes m})$ we have*

$$\inf_{\substack{|v\rangle\in\mathcal{H} \\ \langle v|v\rangle=1}} F(T(|v\rangle\langle v|^{\otimes n}), |v\rangle\langle v|^{\otimes m}) \leq \frac{d[n]}{d[m]},$$

where

$$d[k] = \binom{k+d-1}{k},$$

is the dimension of the symmetric subspace $\mathcal{H}^{\vee k}$, where $d = \dim(\mathcal{H})$. Moreover, there exists a quantum channel T attaining this bound.

Proof. Using that $T(|v\rangle\langle v|^{\otimes n}) \leq T(P^n_{sym})$ by positivity, we can estimate

$$\begin{aligned} \inf_{|v\rangle\in\mathcal{H}} \langle T(|v\rangle\langle v|^{\otimes n}), |v\rangle\langle v|^{\otimes m}\rangle_{HS} &\leq \inf_{|v\rangle\in\mathcal{H}} \langle T(P^n_{sym}), |v\rangle\langle v|^{\otimes m}\rangle_{HS} \\ &\leq \int_{\mathcal{U}(\mathcal{H})} \langle T(P^n_{sym}), \left(U|0\rangle\langle 0|U^\dagger\right)^{\otimes m}\rangle_{HS} d\eta(U). \end{aligned}$$

By a result from the previous lecture we have

$$\frac{P^m_{sym}}{\mathrm{Tr}\left[P^m_{sym}\right]} = \int_{\mathcal{U}(\mathcal{H})} \left(U|0\rangle\langle 0|U^\dagger\right)^{\otimes m} d\eta(U),$$

and we obtain

$$\inf_{|v\rangle\in\mathcal{H}} \langle T(|v\rangle\langle v|^{\otimes n}), |v\rangle\langle v|^{\otimes m}\rangle_{HS} \leq \langle T(P^n_{sym}), \frac{P^m_{sym}}{\mathrm{Tr}\left[P^m_{sym}\right]}\rangle_{HS} \leq \frac{\mathrm{Tr}\left[T(P^n_{sym})\right]}{\mathrm{Tr}\left[P^m_{sym}\right]} = \frac{d[n]}{d[m]}.$$

To attain this bound, we consider the quantum channel $T : B(\mathcal{H}^{\otimes n}) \to B(\mathcal{H}^{\otimes m})$ given by

$$T(X) = \frac{d[n]}{d[m]} P^m_{sym} \left(X \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right) P^m_{sym} + \langle \mathbb{1}_{\mathcal{H}}^{\otimes n} - P^n_{sym}, X\rangle_{HS}\sigma,$$

where $\sigma \in D(\mathcal{H}^{\otimes m})$ is arbitrary. Note that T is a quantum channel since

$$\mathrm{Tr}\left[P^m_{sym}\left(X \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right) P^m_{sym}\right] = \mathrm{Tr}\left[P^m_{sym}\left(X \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right)\right] = \frac{d[m]}{d[n]} \mathrm{Tr}\left[P^n_{sym} X\right],$$

where we used that

$$\left(\mathrm{id}_{\mathcal{H}} \otimes \mathrm{Tr}^{\otimes(m-n)}\right)\left(P^m_{sym}\right) = d[m]\int_{\mathcal{U}(\mathcal{H})} (U|0\rangle\langle 0|U^\dagger)^{\otimes n} d\eta(U) = \frac{d[m]}{d[n]} P^n_{sym}.$$

Finally, we note that for any pure state $|v\rangle \in \mathcal{H}$ we have

$$\langle T(|v\rangle\langle v|^{\otimes n}), |v\rangle\langle v|^{\otimes m}\rangle_{HS} = \frac{d[n]}{d[m]} \mathrm{Tr}\left[\left(|v\rangle\langle v|^{\otimes n} \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right) P^m_{sym}|v\rangle\langle v|^{\otimes m} P^m_{sym}\right] = \frac{d[n]}{d[m]},$$

since $P^m_{sym}|v\rangle\langle v|^{\otimes m}P^m_{sym} = |v\rangle\langle v|^{\otimes m}$. □

For $N = 2$, the quantitative version of the no-cloning theorem shows that

$$\inf_{\substack{|v\rangle\in\mathcal{H} \\ \langle v|v\rangle = 1}} F(T(|v\rangle\langle v|), |v\rangle\langle v|^{\otimes 2}) \leq \frac{2}{d+1},$$

for any quantum channel[1] $T : B(\mathcal{H}) \to B(\mathcal{H}\otimes\mathcal{H})$. Hence, there are pure states $|v\rangle\langle v| \in \mathrm{Proj}\,(\mathcal{H})$ whose image under T is far away from the product $|v\rangle\langle v| \otimes |v\rangle\langle v|$ in fidelity. If you look careful at the proof of the previous theorem, you can observe that a slightly stronger statement holds: Even the average fidelity between the quantum states $T(|v\rangle\langle v|)$ and the pure states $|v\rangle\langle v|^{\otimes 2}$ when averaging over pure states is low (provided that d is large). From either result we conclude that it is impossible to exactly copy every pure state using a fixed quantum channel. Remarkably, the theorem also identifies an optimal cloning channel, which comes as close as possible to a copying device.

3 The Chiribella identity and quantum de-Finetti theorem

There is even more to say about the structure of the symmetric subspace and the no-cloning problem. In the final part of this lecture, we will discuss a few additional observations which will lead to the quantum de-Finetti theorem. To prove this result, we will need to consider a subspace of symmetric operators:

3.1 Bose-symmetric operators

We start with a definition:

Definition 3.1 (Bose-symmetric operators)**.** *We will call operators in $B\left(\mathcal{H}^{\vee N}\right)$* Bose-symmetric*. Sometimes, we will tacitly view the Bose-symmetric operators as a subspace of $B(\mathcal{H})^{\vee N}$.*

Examples of Bose-symmetric operators include P^N_{sym} and operators of the form $|v\rangle\langle w|^{\otimes N}$ for $|v\rangle, |w\rangle \in \mathcal{H}$. Note that $B\left(\mathcal{H}^{\vee N}\right) \subsetneq B(\mathcal{H})^{\vee N}$ since we have, for example, that

$$\mathbb{1}_{\mathcal{H}}^{\otimes N} \in B(\mathcal{H})^{\vee N} \setminus B\left(\mathcal{H}^{\vee N}\right).$$

The following lemma is left as an exercise:

Lemma 3.2. *For any complex Euclidean space $\mathcal{H}$ we have*

$$B\left(\mathcal{H}^{\vee N}\right) = \mathrm{span}_{\mathbb{C}}\{|v\rangle\langle v|^{\otimes N} \; : \; |v\rangle \in \mathcal{H}\},$$

and

$$B\left(\mathcal{H}^{\vee N}\right)_{sa} = \mathrm{span}_{\mathbb{R}}\{|v\rangle\langle v|^{\otimes N} \; : \; |v\rangle \in \mathcal{H}\}.$$

Proof. Exercise. □

[1] and even unphysical positive trace-preserving maps

3.2 Cloning and the measure-prepare map

In the quantitative version of the no-cloning theorem we introduced the *optimal cloning map*, which we can restrict to the space $B(\mathcal{H}^{\vee n})$: Let $\text{clone}_{n\to m} : B(\mathcal{H}^{\vee n}) \to B(\mathcal{H}^{\vee m})$ denote the map given by

$$\text{clone}_{n\to m}(X) = \frac{d[n]}{d[m]} P^m_{sym} \left(X \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)} \right) P^m_{sym},$$

where we denote the dimension of the symmetric subspace $\mathcal{H}^{\vee k}$ by

$$d[k] := \binom{k+d-1}{k},$$

with $d = \dim(\mathcal{H})$. The map $\text{clone}_{n\to m}$ is the optimal cloning map from Theorem 2.1 restricted to the space $B(\mathcal{H}^{\vee n})$. It can also be checked that this map coincides (up to a normalization factor) with the adjoint $\text{Tr}^*_{m\to n}$ of the partial trace map $\text{Tr}_{m\to n} : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$. We will need another linear map on the symmetric operators: The *measure-prepare map* $\text{MP}_{m\to n} : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ is given by

$$\text{MP}_{m\to n}(X) = d[m] \int_{\mathcal{U}(\mathcal{H})} \langle \phi_U^{\otimes m} | X | \phi_U^{\otimes m} \rangle |\phi_U\rangle\langle\phi_U|^{\otimes n} d\eta(U),$$

where $|\phi_U\rangle = U|0\rangle$ for any $U \in \mathcal{U}(\mathcal{H})$. We will need the following lemma:

Lemma 3.3. *For any $m \geq n$ the maps $\text{MP}_{m\to n} : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ and $\text{clone}_{n\to m} : B(\mathcal{H}^{\vee n}) \to B(\mathcal{H}^{\vee m})$ are quantum channels.*

Proof. It is clear that these maps are completely positive. To see that they are trace-preserving we can compute

$$\text{Tr}\left[\text{MP}_{m\to n}(X)\right] = d[m] \int_{\mathcal{U}(\mathcal{H})} \langle \phi_U^{\otimes m} | X | \phi_U^{\otimes m} \rangle d\eta(U) = \text{Tr}\left[P^m_{sym} X\right] = \text{Tr}\left[X\right],$$

for every $X \in B(\mathcal{H}^{\vee m})$. Similarly, for every $Y \in B(\mathcal{H}^{\vee n})$ we have

$$\text{Tr}\left[\text{clone}_{n\to m}(Y)\right] = \frac{d[n]}{d[m]} \text{Tr}\left[P^m_{sym}\left(Y \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right)\right] = \text{Tr}\left[P^n_{sym} Y\right] = \text{Tr}\left[Y\right],$$

as in the proof of Theorem 2.1. □

There is a remarkable identity connecting the optimal cloning maps to the measurement-prepare maps:

Theorem 3.4 (Chiribella identity)**.** *For any $m \geq n$ we have*

$$\text{MP}_{m\to n} = \frac{d[m]}{d[m+n]} \sum_{s=0}^{n} \frac{d[n]}{d[s]} \frac{\binom{m}{s}\binom{n}{s}}{\binom{m+n}{s}} \text{clone}_{s\to n} \circ \text{Tr}_{m\to s}.$$

Proof. Exercises. □

Why is the Chiribella identity useful? Let us consider the coefficient of the last term on the right-hand side (i.e., the term for $s = n$):

$$\frac{d[m]}{d[m+n]} \frac{\binom{m}{n}}{\binom{m+n}{n}} = \frac{m!(m+d-1)!}{(m-n)!(m+n+d-1)!} \geq \left(1 - \frac{d+n}{d+m}\right)^n \geq 1 - \frac{n(d+n)}{m+d}.$$

Since $\text{clone}_{n\to n} = \text{id}_{B(\mathcal{H}^{\vee n})}$, we conclude that

$$\text{MP}_{m\to n} = (1 - \epsilon_{m,n,d}) \text{Tr}_{m\to n} + \epsilon_{m,n,d} R,$$

for some quantum channel $R : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ and some

$$\epsilon_{m,n,d} \leq \frac{n(d+n)}{m+d}.$$

As a consequence we obtain the following theorem:

Theorem 3.5 (Quantum de-Finetti theorem)**.** *For any $m \geq n$ and any pure quantum state $|\psi\rangle \in \mathcal{H}^{\vee m}$ there exists a quantum state*

$$\sigma \in conv\{|v\rangle\langle v|^{\otimes n} \ : \ |v\rangle \in \mathcal{H}, \langle v|v\rangle = 1\},$$

such that

$$\| \operatorname{Tr}_{m \to n} [|\psi\rangle\langle\psi|] - \sigma\|_1 \leq \frac{n(d+n)}{m+d}.$$