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

Lecture 14: The symmetric subspace and Schur-Weyl duality

Lecturer: Alexander Müller-Hermes

In the previous lecture, we have constructed the Haar measure on the unitary group. This measure can be used to symmetrize quantum states and quantum channels in various ways. Here, we will give an introduction to some of these symmetries and how they give rise to two families of quantum states known as Werner states (after Reinhard Werner, who first introduced them) and isotropic quantum states. These families have nice properties and they play a central role in the manipulation of quantum information.

1 Permutations of tensor factors

Recall the symmetric group S_N consisting of permutations of N elements, i.e., bijections $\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$. Let $\mathcal{H}$ denote a complex Euclidean space. The group S_N acts naturally on the tensor product $\mathcal{H}^{\otimes N}$ by the (unitary) representation $S_N \ni \sigma \mapsto U_\sigma \in \mathcal{U}\left(\mathcal{H}^{\otimes N}\right)$ defined as

$$U_\sigma \left(|v_1\rangle \otimes \cdots \otimes |v_N\rangle\right) = |v_{\sigma^{-1}(1)}\rangle \otimes \cdots \otimes |v_{\sigma^{-1}(N)}\rangle,$$

and extended linearly. The following properties can be verified easily:

- For any $\sigma_1, \sigma_2 \in S_N$ we have $U_{\sigma_1} U_{\sigma_2} = U_{\sigma_1 \circ \sigma_2}$.
- For any $\sigma \in S_N$ we have $U_\sigma^{-1} = U_{\sigma^{-1}} = U_\sigma^\dagger = U_\sigma^T$, where the transpose is in the computational basis.

1.1 The symmetric subspace

Throughout this section let $\mathcal{H}$ denote a complex Euclidean space. We will need the following subspace of $\mathcal{H}^{\otimes N}$:

Definition 1.1 (Symmetric subspace)**.** *For any $N \in \mathbb{N}$, we define*

$$\mathcal{H}^{\vee N} = \{|\psi\rangle \in \mathcal{H}^{\otimes N} \ : \ U_\sigma|\psi\rangle = |\psi\rangle \text{ for all } \sigma \in S_N\}.$$

In the following, we will prove some elementary properties of the symmetric subspace that will become useful later. For this, let $P^N_{\text{sym}} \in \text{Proj}\left(\mathcal{H}^{\otimes N}\right)$ denote the orthogonal projection onto $\mathcal{H}^{\vee N}$, which we will also call the *symmetric projection*. The next lemma is an easy exercise:

Lemma 1.2. *For any $N \in \mathbb{N}$ we have*

$$P^N_{sym} = \frac{1}{N!} \sum_{\sigma \in S_N} U_\sigma.$$

Proof. It is easy to check that $\left(P^N_{\text{sym}}\right)^\dagger = P^N_{\text{sym}}$ since $U_\sigma^\dagger = U_{\sigma^{-1}}$ and S_N is a group. We can also check that $U_\sigma \circ P^N_{\text{sym}} = P^N_{\text{sym}} \circ U_\sigma = P^N_{\text{sym}}$ for any $\sigma \in S_N$, which implies that $\left(P^N_{\text{sym}}\right)^2 = P^N_{\text{sym}}$ and that $\text{Im}\left(P^N_{\text{sym}}\right) \subseteq \mathcal{H}^{\vee N}$. In conclusion, P^N_{sym} is an orthogonal projection and clearly we have $\text{Im}\left(P^N_{\text{sym}}\right) = \mathcal{H}^{\vee N}$.

□

Next, we will find an orthonormal basis for $\mathcal{H}^{\vee N}$. For this let $d = \dim(\mathcal{H})$ and let $\{|1\rangle, \ldots, |d\rangle\} \subset \mathcal{H}$ denote the computational basis. Consider the function $\tau : \{1, \ldots, d\}^N \to \{0, 1, \ldots, N\}^d$ mapping each string $s \in \{1, \ldots, d\}^N$ of length N to its *type* given by

$$\tau(s) = (\#\{i \ : \ s_i = 1\}, \#\{i \ : \ s_i = 2\}, \ldots, \#\{i \ : \ s_i = d\}) \, .$$

For each $N, d \in \mathbb{N}$, we define the set

$$\mathcal{T}_{d,N} = \{t \in \{0, 1, \ldots, N\}^d \ : \ t_1 + \cdots + t_d = N\},$$

of all possible types a string $s \in \{1, \ldots, d\}^N$ could have, and we denote by $\tau^{-1}(t) \subset \{1, \ldots, d\}^N$ the set of all strings compatible with the type $t \in \mathcal{T}_{d,N}$. The following lemma is an exercise in combinatorics:

Lemma 1.3. *For any $d, N \in \mathbb{N}$ we have*

$$|\mathcal{T}_{d,N}| = \binom{d+N-1}{N},$$

and

$$|\tau^{-1}(t)| = \binom{N}{t} := \frac{N!}{t_1! t_2! \cdots t_d!},$$

for any $t \in \{0, 1, \ldots, N\}^d$.

Proof. The proof of the second statement is easy. To prove the first statement we can use the stars-and-bars graphical notation (see Figure 1)

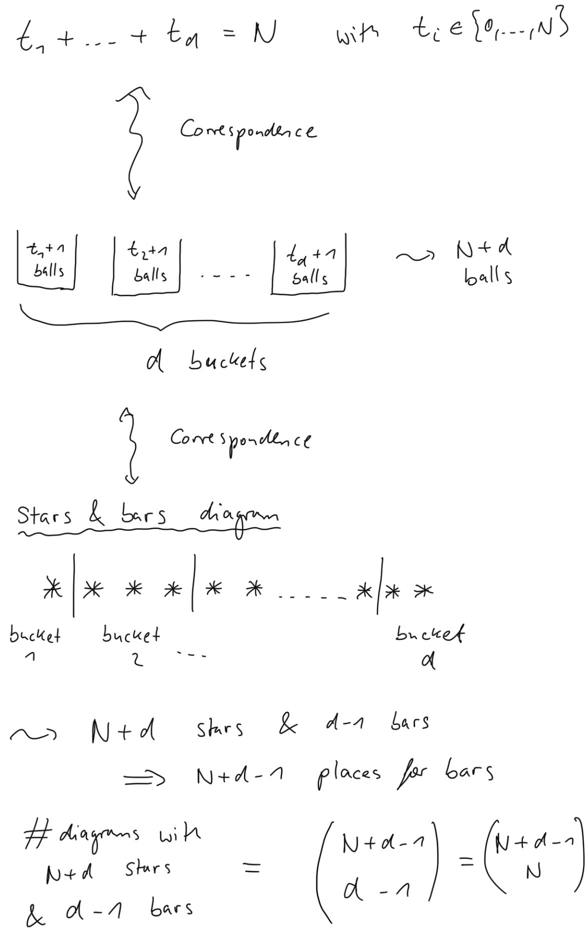

Figure 1: Proof by stars and bars.

$\square$

Now, we can find two ways of representing the symmetric subspace:

Theorem 1.4. *Let $\mathcal{H}$ denote a complex Euclidean space of dimension $d \in \mathbb{N}$ and let $N \in \mathbb{N}$. For any $t \in \mathcal{T}_{d,N}$ we define a vector*

$$|b(t)\rangle = \frac{1}{\sqrt{\binom{N}{t}}} \sum_{s \in \tau^{-1}(t)} |s_1\rangle \otimes \cdots \otimes |s_N\rangle.$$

Then, $\{|b(t)\rangle \ : \ t \in \mathcal{T}_{d,N}\}$ is an orthonormal basis of $\mathcal{H}^{\vee N}$. Moreover, we have

$$\dim(\mathcal{H}^{\vee N}) = \binom{d+N-1}{N}.$$

Proof. Since the type of a string s is invariant under exchanging its order, it is easy to see that $|b(t)\rangle \in \mathcal{H}^{\vee N}$ for any $t \in \mathcal{T}_{d,N}$. On the other hand, we clearly have

$$P^N_{\text{sym}}\left(|s_1\rangle \otimes \cdots \otimes |s_N\rangle\right) = |b(t)\rangle,$$

whenever $\tau(s) = t$. Therefore, we conclude that

$$\mathcal{H}^{\vee N} = \text{Im}\left(P^N_{\text{sym}}\right) \subseteq \text{span}\{|b(t)\rangle \ : \ t \in \mathcal{T}_{d,N}\} \subseteq \mathcal{H}^{\vee N}.$$

This finishes the proof. $\square$

The basis $\{|b(t)\rangle \ : \ t \in \mathcal{T}_{d,N}\}$ can be seen as the standard basis of the symmetric subspace $\mathcal{H}^{\vee N}$, but there is another spanning set that is equality important:

Theorem 1.5. *Let $\mathcal{H}$ denote a complex Euclidean space of dimension $d \in \mathbb{N}$ and let $N \in \mathbb{N}$. We have*

$$\mathcal{H}^{\vee N} = \text{span}\{|v\rangle^{\otimes N} \ : \ |v\rangle \in \mathcal{H}\}.$$

Moreover, for any set $\mathcal{S} \subset \mathbb{C}$ satisfying $|\mathcal{S}| \geq N+1$ we have

$$\mathcal{H}^{\vee N} = \text{span}\{|v\rangle^{\otimes N} \ : \ |v\rangle \in \mathcal{H} \text{ such that } v_i \in \mathcal{S} \text{ for every } i\}.$$

To prove this theorem, we need the following fact:

Theorem 1.6 (Vandermonde matrix)**.** *For distinct numbers $x_1, \ldots, x_N \in \mathbb{C}$ the Vandermonde matrix*

$$V(x_1, \ldots, x_N) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_N \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_N^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{N-1} & x_2^{N-1} & x_3^{N-1} & \cdots & x_N^{N-1} \end{pmatrix}$$

is invertible. In particular, for every $n \in \{0, \ldots, N-1\}$ there exist numbers $\alpha_1^{(n)}, \alpha_2^{(n)}, \ldots, \alpha_N^{(n)} \in \mathbb{C}$ such that

$$\sum_{i=1}^{N} \alpha_i^{(n)} x_i^k = \delta_{nk}.$$

Proof. The determinant of $V(x_1, \ldots, x_N)$ can be computed inductively as

$$\det\left(V(x_1, \ldots, x_N)\right) = \prod_{i<j} (x_j - x_i),$$

which is non-zero if and only if the numbers $x_1, \ldots, x_{N+1} \in \mathbb{C}$ are distinct. $\square$

Proof of Theorem 1.5. Again, it is easy to see that $|v\rangle^{\otimes N} \in \mathcal{H}^{\vee N}$ for any $|v\rangle \in \mathcal{H}$. For the rest of the proof, we fix a subset $\mathcal{S} \subseteq \mathbb{C}$ such that $|\mathcal{S}| \geq N+1$. It remains to show that

$$\mathcal{H}^{\vee N} \subseteq \text{span}\{|v\rangle^{\otimes N} \ : \ |v\rangle \in \mathcal{H} \text{ such that } v_i \in \mathcal{S} \text{ for every } i\}.$$

For $y_1, \ldots, y_d \in \mathcal{S}$ we define

$$|p(y_1, \ldots, y_d)\rangle := \left(\sum_{l=1}^{d} y_l |l\rangle\right)^{\otimes N} \in \text{span}\{|v\rangle^{\otimes N} \ : \ |v\rangle \in \mathcal{H} \text{ such that } v_i \in \mathcal{S} \text{ for every } i\},$$

which can be expanded to

$$|p(y_1, \ldots, y_d)\rangle = \sum_{s \in \mathcal{T}_{d,N}} \sqrt{\binom{N}{s}} y_1^{s_1} \cdots y_d^{s_d} |b(s)\rangle.$$

Now, let $x_1, \ldots, x_{N+1} \in \mathcal{S}$ denote distinct elements. By Lemma 1.6 there are numbers $\alpha_1^{(n)}, \alpha_2^{(n)}, \ldots, \alpha_{N+1}^{(n)} \in \mathbb{C}$ for each $n \in \{0, \ldots, N\}$ such that

$$\sum_{i=1}^{N+1} \alpha_i^{(n)} x_i^k = \delta_{nk},$$

for any $k \in \{0, \ldots, N\}$. Then, we can check that

$$\begin{aligned}\sqrt{\binom{N}{t}} |b(t)\rangle &= \sum_{i_1, \ldots, i_d = 1}^{N+1} \alpha_{i_1}^{(t_1)} \cdots \alpha_{i_d}^{(t_d)} |p(x_{i_1}, \ldots, x_{i_d}\rangle \\ &\in \text{span}\{|v\rangle^{\otimes N} \ : \ |v\rangle \in \mathcal{H} \text{ such that } v_i \in \mathcal{S} \text{ for every } i\},\end{aligned}$$

by linearity of the span. □

1.2 The subspace of symmetric operators

In this section, we will discuss the symmetric subspace of the Hilbert-Schmidt inner product space $B(\mathcal{H}^{\otimes N}) \simeq B(\mathcal{H})^{\otimes N}$, which is a special case of the construction from the previous section. The following lemma is left as an exercise:

Lemma 1.7 (Symmetric operators)**.** *Let $\mathcal{H}$ denote a complex Euclidean space, $N \in \mathbb{N}$ and $X \in B(\mathcal{H}^{\otimes N})$. Then, the following are equivalent:*

1. *We have $X \in B(\mathcal{H})^{\vee N}$.*
2. *For any $\sigma \in S_N$ we have $U_\sigma X U_\sigma^\dagger = X$.*
3. *We have $X \in \text{span}\{Y^{\otimes N} \ : \ Y \in B(\mathcal{H})\}$.*

The third point in the previous lemma is just the representation of the symmetric subspace as the span of tensor powers. However, in the case of symmetric operators we have a strengthening of this fact:

Theorem 1.8. *For any complex Euclidean space $\mathcal{H}$ and any $N \in \mathbb{N}$ we have*

$$B(\mathcal{H})^{\vee N} = \text{span}\{U^{\otimes N} \ : \ U \in \mathcal{U}(\mathcal{H})\}.$$

Proof. By Theorem 1.5, for every $|w\rangle \in \mathcal{H}$ we have

$$|w\rangle^{\otimes N} = \sum_i \lambda_i |v_i\rangle^{\otimes N},$$

for some $\lambda_i \in \mathbb{C}$ and some $|v_i\rangle \in \mathcal{H}$ satisfying $|(v_i)_j| = 1$. We conclude that

$$D^{\otimes N} = \sum_i \lambda_i U_i^{\otimes N},$$

where $D \in B(\mathcal{H})$ is the operator containing the entries of $|w\rangle$ on its diagonal (in the computational basis) and U_i is the unitary diagonal operator containing the entries of $|v_i\rangle$ on its diagonal (again in the computational basis). This shows that any diagonal operator $D \in B(\mathcal{H})$ satisfies

$$D^{\otimes N} \in \text{span}\{U^{\otimes N} \ : \ U \in \mathcal{U}(\mathcal{H})\}.$$

Consider now an arbitrary operator $Y \in B(\mathcal{H})$, which can be written as

$$Y = VDW,$$

for a diagonal operator $D \in B(\mathcal{H})$ and unitary operators $V, W \in \mathcal{U}(\mathcal{H})$. By the previous observation, we conclude that

$$Y^{\otimes N} = V^{\otimes N} D^{\otimes N} W^{\otimes N} \in \text{span}\{U^{\otimes N} \ : \ U \in \mathcal{U}(\mathcal{H})\}.$$

Since this holds for any operator $Y \in B(\mathcal{H})$ we conclude by Lemma 1.7 that

$$B(\mathcal{H})^{\vee N} = \text{span}\{Y^{\otimes N} \ : \ Y \in B(\mathcal{H})\} \subseteq \text{span}\{U^{\otimes N} \ : \ U \in \mathcal{U}(\mathcal{H})\}.$$

The other inclusion is trivial. □

The previous theorem has an important consequence: The symmetric subspace $\mathcal{H}^{\vee N}$ is an irreducible representation of $\mathcal{U}\left(\mathbb{C}^d\right) \ni U \mapsto U^{\otimes N}$. Since we want to keep the presentation selfcontained we will state this result in elementary terms:

Corollary 1.9. *Any subspace $\mathcal{S} \subseteq \mathcal{H}^{\vee N}$ satisfying $U^{\otimes N}(\mathcal{S}) \subseteq \mathcal{S}$ for any $U \in \mathcal{U}(\mathcal{H})$, i.e., any* invariant subspace, *satisfies either $\mathcal{S} = \{0\}$ or $\mathcal{S} = \mathcal{H}^{\vee N}$.*

Proof. By Theorem 1.8 any invariant subspace $\mathcal{S} \subseteq \mathcal{H}^{\vee N}$ satisfies $X(\mathcal{S}) \subseteq \mathcal{S}$ for any $X \in B(\mathcal{H})^{\vee N} = \text{span}\{U^{\otimes N} \ : \ U \in \mathcal{U}(\mathcal{H})\}$. If $|\psi\rangle \in \mathcal{S}$ is non-zero, we could consider the operator $X = |\phi\rangle\langle\psi| \in B(\mathcal{H})^{\vee N}$ for any $|\phi\rangle \in \mathcal{H}^{\vee N}$. Invariance of $\mathcal{S}$ then implies that $|\phi\rangle \in \mathcal{S}$ as well, and we conclude that $\mathcal{S} = \mathcal{H}^{\vee N}$ since the choice of $|\phi\rangle$ was arbitrary.

□

An important consequence of this corollary is the following theorem giving a useful representation of the symmetric projection:

Theorem 1.10. *For any Euclidean space $\mathcal{H}$ and any $N \in \mathbb{N}$ we have*

$$\frac{P^N_{sym}}{\text{Tr}\left[P^N_{sym}\right]} = \int_{\mathcal{U}(\mathcal{H})} \left(U|\phi\rangle\langle\phi|U^\dagger\right)^{\otimes N} d\eta(U),$$

for any pure quantum state $|\phi\rangle \in \mathcal{H}$.

Note that we could use Schur's lemma to prove this theorem. To keep the discussion selfcontained, we will now cast the general (and short) proof of Schur's lemma into the setting at hand.

Proof. For some pure quantum state $|\phi\rangle \in \mathcal{H}$, we set

$$X = \int_{\mathcal{U}(\mathcal{H})} \left(U|\phi\rangle\langle\phi|U^\dagger\right)^{\otimes N} d\eta(U) \in B\left(\mathcal{H}\right)^{\vee N}.$$

We observe that X is selfadjoint, and that $X|\psi\rangle = 0$ whenever $|\psi\rangle \in (\mathcal{H}^{\vee N})^{\perp}$. Now, consider an eigenvalue $\lambda \in \mathbb{R}\setminus\{0\}$ and note that

$$\mathcal{S} = \{|\psi\rangle \in \mathcal{H}^{\vee N} \ : \ \left(X - \lambda P^N_{sym}\right)|\psi\rangle = 0\} \neq \{0\}.$$

Using that $\left[X, U^{\otimes N}\right] = 0$ for any $U \in \mathcal{U}\left(\mathcal{H}\right)$ we find that

$$\left(X - \lambda P^N_{sym}\right) U^{\otimes N}|\psi\rangle = U^{\otimes N}\left(X - \lambda P^N_{sym}\right)|\psi\rangle = 0,$$

and hence we have $U^{\otimes N}(\mathcal{S}) \subseteq \mathcal{S}$ for any $U \in \mathcal{U}\left(\mathcal{H}\right)$. By Theorem 1.9 we conclude that $\mathcal{S} = \mathcal{H}^{\vee N}$ (note that $\mathcal{S}$ contains at least one non-zero vector by definition) and hence that

$$X|\psi\rangle = \lambda|\psi\rangle,$$

for any $|\psi\rangle \in \mathcal{H}^{\vee N}$. We conclude that $X = \lambda P^N_{sym}$ and, since $\mathrm{Tr}\left[X\right] = 1$, the proof is finished. □

2 Interplay between different symmetries

2.1 The double commutant theorem

We will need the following lemma:

Lemma 2.1. *Let $\mathcal{H}$ denote a complex Euclidean space and $\mathcal{V} \subseteq \mathcal{H}$ a subspace. For any operator $X \in B(\mathcal{H})$ the following are equivalent:*

1. *We have $X\mathcal{V} \subseteq \mathcal{V}$ and $X^\dagger\mathcal{V} \subseteq \mathcal{V}$.*
2. *We have $[X, \Pi_\mathcal{V}] = 0$, where $\Pi_\mathcal{V}$ denotes the orthogonal projection onto $\mathcal{V}$.*

Proof. The second statement implies that

$$X|v\rangle = X\Pi_\mathcal{V}|v\rangle = \Pi_\mathcal{V}X|v\rangle \in \mathcal{V},$$

for any $|v\rangle \in \mathcal{V}$. By taking adjoints, the same holds for the operator $X^\dagger$ instead. We conclude that the first statement follows from the second.

Assume now that the first statement holds, and note that we have

$$\Pi_\mathcal{V}X|v\rangle = X|v\rangle = X\Pi_\mathcal{V}|v\rangle,$$

for any $|v\rangle \in \mathcal{V}$. Now, consider $|w\rangle \in \mathcal{V}^\perp$ and note that

$$\langle v|X|w\rangle = \langle X^\dagger v||w\rangle = 0,$$

for any $|v\rangle \in \mathcal{V}$, which implies that $X|w\rangle \in \mathcal{V}^\perp$. Any $|u\rangle \in \mathcal{H}$ can then be written as $|u\rangle = |v\rangle + |w\rangle$ with $|v\rangle \in \mathcal{V}$ and $|w\rangle \in \mathcal{V}^\perp$, and we have

$$X\Pi_\mathcal{V}|u\rangle = X\Pi_\mathcal{V}|v\rangle = \Pi_\mathcal{V}X|v\rangle = \Pi_\mathcal{V}X(|v\rangle + |w\rangle) = \Pi_\mathcal{V}X|u\rangle.$$

We conclude that $[X, \Pi_\mathcal{V}] = 0$, which is the second statement. □

Theorem 2.2 (The double commutant theorem light)**.** *Let $\mathcal{H}$ denote a complex Euclidean space and $\mathcal{A} \subseteq B(\mathcal{H})$ a $\dagger$-closed subalgebra containing $\mathbb{1}_{\mathcal{H}}$. Then, we have*

$$\mathcal{A}'' = \mathcal{A},$$

where $\mathcal{S}'$ denotes the commutant of an algebra $\mathcal{S}$, i.e., the set of operators commuting with all operators in $\mathcal{S}$.

Proof. It is clear that

$$\mathcal{A} \subseteq \mathcal{A}'',$$

and we only have to show the other inclusion. Consider the subspace

$$\mathcal{V} = \{\text{vec}\, X \ : \ X \in \mathcal{A}\} \subseteq \mathcal{H} \otimes \mathcal{H},$$

obtained by vectorizing the operators in $\mathcal{A}$. Since $\mathcal{A}$ is a $\dagger$-closed algebra we can use the necklace identity to show that

$$(\mathbb{1}_{\mathcal{H}} \otimes X)\mathcal{V} \subseteq \mathcal{V}, \quad \text{and} \quad (\mathbb{1}_{\mathcal{H}} \otimes X^{\dagger})\mathcal{V} \subseteq \mathcal{V},$$

for any $X \in \mathcal{A}$. By Lemma 2.1 we conclude that

$$[\mathbb{1}_{\mathcal{H}} \otimes X, \Pi_{\mathcal{V}}] = 0,$$

for any $X \in \mathcal{A}$. This implies that $\Pi_{\mathcal{V}} \in \mathcal{B}'$ for

$$\mathcal{B} = \{\mathbb{1}_{\mathcal{H}} \otimes X \ : \ X \in \mathcal{A}\}.$$

Consider now some $Y \in \mathcal{A}''$. We will show that $\mathbb{1}_{\mathcal{H}} \otimes Y \in \mathcal{B}''$ implying that

$$[\mathbb{1}_{\mathcal{H}} \otimes Y, \Pi_{\mathcal{V}}] = 0,$$

and by Lemma 2.1 that $(\mathbb{1}_{\mathcal{H}} \otimes Y)\mathcal{V} \subseteq \mathcal{V}$. Since $\mathcal{A}$ contains $\mathbb{1}_{\mathcal{H}}$ we conclude that

$$(\mathbb{1}_{\mathcal{H}} \otimes Y)\, \text{vec}(\mathbb{1}_{\mathcal{H}}) = \text{vec}(Y) \in \mathcal{V},$$

and hence that $Y \in \mathcal{A}$ finishing the proof.

It remains to show that $\mathbb{1}_{\mathcal{H}} \otimes Y \in \mathcal{B}''$ whenever $Y \in \mathcal{A}''$. This is not difficult: Any operator $Z \in B(\mathcal{H} \otimes \mathcal{H})$ can be written as

$$Z = \sum_{i,j} |i\rangle\langle j| \otimes Z_{ij},$$

with $Z_{ij} \in B(\mathcal{H})$ for all i, j. If $Z \in \mathcal{B}'$, then it is easy to see that $Z_{ij} \in \mathcal{A}'$ for any i, j, and that $[Z, \mathbb{1}_{\mathcal{H}} \otimes Y] = 0$ for any $Y \in \mathcal{A}''$. The proof is finished. □

2.2 Schur-Weyl duality light

Theorem 2.3. *Let $\mathcal{H}$ denote a complex Euclidean space and let $N \in \mathbb{N}$. For $X \in B\left(\mathcal{H}^{\otimes N}\right)$, the following are equivalent:*

1. *We have $\left[X, Y^{\otimes N}\right] = 0$ for any $Y \in B(\mathcal{H})$.*
2. *We have $\left[X, U^{\otimes N}\right] = 0$ for any $U \in \mathcal{U}(\mathcal{H})$.*
3. *We have*

$$X \in \text{span}\{U_\sigma \ : \ \sigma \in S_N\}.$$

Proof. Both the first and the second statements are equivalent to

$$X \in \left(B\left(\mathcal{H}\right)^{\vee N}\right)'.$$

We will now show that

$$\left(B\left(\mathcal{H}\right)^{\vee N}\right)' = \mathrm{span}\{U_\sigma \ : \ \sigma \in S_N\},$$

which finishes the proof. First, we note that

$$\mathcal{A} = \mathrm{span}\{U_\sigma \ : \ \sigma \in S_N\},$$

is a †-closed algebra containing $\mathbb{1}_{\mathcal{H}} = U_{\mathrm{id}}$. Then, we observe that $X \in B(\mathcal{H}^{\otimes N})$ is contained in $B\left(\mathcal{H}\right)^{\vee N}$ if and only if $[X, U_\sigma] = 0$ for every $\sigma \in S_N$. This shows that

$$B\left(\mathcal{H}\right)^{\vee N} = \mathcal{A}'.$$

By taking commutators on both sides of this equation and using the double commutant theorem we conclude that

$$\mathcal{A} = \left(B\left(\mathcal{H}\right)^{\vee N}\right)',$$

which finishes the proof. □