Formalization of Weingarten Calculus

Melody Lee Yanting Teng

June 24, 2026

Chapter 1

Schur Weyl Duality

1.1 Operator Space

Suppose $\mathcal{X} = \mathbb{C}^{[d]}$ and $\mathcal{Y} = \mathbb{C}^{[d]}$ where $d \in \mathbb{N}$. Let the set of linear operators be $\mathcal{L}(\mathcal{X}, \mathcal{Y})$. When $\mathcal{Y} = \mathcal{X}$, let the set of linear operators be $\mathcal{L}(\mathcal{X})$.

We briefly restate some relevant definitions and properties of linear operators that we will use in the subsequent sections.

Remark 1.1.1. For any pair of operators $X, Y \in \mathcal{L}(\mathcal{X})$, the Lie bracket $[X, Y] \in \mathcal{L}(\mathcal{X})$ is defined as

$$[X, Y] = XY - YX, \tag{1.1}$$

such that $[X, Y] = 0$ if and only if X and Y commute.

Remark 1.1.2. Let $\mathcal{A} \subseteq \mathcal{L}(\mathcal{X})$ be a subalgebra of $\mathcal{L}(\mathcal{X})$. The commutant of $\mathcal{A}$ is given by

$$\mathrm{Comm}(\mathcal{A}) = \{Y \in \mathcal{L}(\mathcal{X}) : [X, Y] = 0 \text{ for all } X \in \mathcal{A}\}. \tag{1.2}$$

Definition 1.1.3 (Diagonal operators)**.** An operator $X \in \mathcal{L}(\mathcal{X})$ is a diagonal operator if $X_{a,b} = 0$ for all $a, b \in [d]$ where $a \neq b$. For a given vector $u \in \mathcal{X}$, we can define a diagonal operator $\mathrm{Diag}(u) \in \mathcal{L}(\mathcal{X})$ to denote the diagonal operator whose diagonal entries are given by the entries of u. That is, we have

$$\mathrm{Diag}(u)_{a,b} = \begin{cases} u_a & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases} \tag{1.3}$$

Remark 1.1.4 (Projection operators). Let Π denote the project operator onto a subspace $\mathcal{V}$. Then Π is a linear operator that satisfies the following properties:

- $\Pi^2 = \Pi$, the idempotent property; and
- $\Pi^* = \Pi$, the self-adjoint property.

Let the collection of all projection operators be denoted $\mathrm{Proj}(\mathcal{X})$. There is a uniquely defined projection operator $\Pi \in \mathrm{Proj}(\mathcal{X})$ such that its image $\mathrm{Im}(\Pi) = \mathcal{V}$. When necessary, we denote this projection operator as $\Pi_{\mathcal{V}}$ to indicate the subspace $\mathcal{V}$ onto which it projects.

Remark 1.1.5 (Isometries). An operator $\mathcal{A} \in \mathcal{L}(\mathcal{X}, \mathcal{Y})$ is an isometry if it satisfies the condition

$$\mathcal{A}^* \mathcal{A} = I_{\mathcal{X}}, \tag{1.4}$$

which is equivalent to preserving the Euclidean norm of vectors in $\mathcal{X}$, i.e., $\|\mathcal{A}|\psi\rangle\| = \||\psi\rangle\|$ for all $|\psi\rangle \in \mathcal{X}$.

Remark 1.1.6 (Unitary operators). Denote the set of isometries that map $\mathcal{X}$ to itself as the set of unitary operators $U(\mathcal{X})$. Every unitary operator $U \in U(\mathcal{X})$ is necessarily invertible and satisfies the normal condition

$$UU^* = U^*U = I_{\mathcal{X}}. \tag{1.5}$$

1.2 Symmetric subspaces

Definition 1.2.1 (Symmetric subspace of linear operators)**.** The symmetric subspace of linear operators $\mathcal{L}(\mathcal{X})^{\otimes k}$ is the set of all operators $X \in \mathcal{L}(\mathcal{X}^{\otimes k})$ that remain unchanged (invariant) under the permutation W_π. That is,

$$\mathcal{L}(\mathcal{X})^{\otimes k} = \{X \in \mathcal{L}(\mathcal{X}^{\otimes k}) : X = W_\pi X W_\pi^* \text{ for all } \pi \in S_k\}. \tag{1.6}$$

Remark 1.2.2. Let S_k denote the symmetric group. Then given $\pi \in S_k$, the permutation matrix (operator) $V_d(\pi)$ is the unitary matrix that satisfies

$$W_\pi |\psi_1\rangle \otimes ... |\psi_k = |\psi_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes |\psi_{\pi^{-1}(k)}\rangle \tag{1.7}$$

for all $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathbb{C}^d$.

Definition 1.2.3 (Standard computational basis of linear operators)**.** The standard computational basis of linear operators $\{E_{i,j}\}_{i,j\in[d]}$ is defined as the set of d^2 operators in $\mathcal{L}(\mathcal{X})$ such that

$$E_{i,j} = |i\rangle\langle j| \tag{1.8}$$

for all $i, j \in [d]$, where $\{|i\rangle\}_{i\in[d]}$ is the standard computational basis of $\mathcal{X}$.

Definition 1.2.4 (Operator-vector correspondence)**.** The operator-vector correspondence is a bijective mapping between the set of linear operators $\mathcal{L}(\mathcal{X})$ and the tensor product space $\mathcal{X} \otimes \mathcal{X}$ defined as

$$\text{vec} : \mathcal{L}(\mathcal{X}) \to \mathcal{X} \otimes \mathcal{X}, \quad E_{i,j} \mapsto |i\rangle \otimes |j\rangle \text{ for all } i, j \in [d]. \tag{1.9}$$

One relevant identity we use is that for $A_0, A_1, B \in \mathcal{L}(\mathcal{X})$,

$$(A_0 \otimes A_1)\text{vec}(B) = \text{vec}(A_0 B A_1^{\mathrm{T}}). \tag{1.10}$$

1.3 Permutation Invariance and Properties of Unitarily Invariant Measures

Theorem 1.3.1 (Tensor power span theorem)**.** *Let k be a positive integer, and let $X \in \mathbb{C}^[d]$. For any set $\mathcal{A} \subseteq \mathbb{C}$ satisfying $|\mathcal{A}| \geq k+1$, it holds that*

$$Span\{v^{\otimes k} : v \in \mathcal{A}^{[d]}\} = \mathcal{X}^{\otimes k}. \tag{1.11}$$

Proposition 1.3.2 (Symmetric subspace and span of tensor product space)**.** *Let $\mathcal{X}$ be a complex Euclidean space and k be a positive integer. Then the following statements are equivalent:*

1. $X \in \mathcal{L}(\mathcal{X})^{\otimes k}$.

2. *For $V \in U(\mathcal{X}^{\otimes k} \otimes \mathcal{X}^{\otimes k}, (\mathcal{X} \otimes \mathcal{X})^{\otimes k})$ being the isometry defined by*

$$V\,vec(Y_1 \otimes \cdots \otimes Y_k) = vec(Y_1) \otimes \ldots vec(Y_n) \tag{1.12}$$

   holding for all $Y_1, \ldots, Y_k \in \mathcal{L}(\mathcal{X})$, one has that

$$V\,vec(X) \in (\mathcal{X} \otimes \mathcal{X})^{\otimes k}. \tag{1.13}$$

3. *$X \in Span\{Y^{\otimes k} : Y \in \mathcal{L}(\mathcal{X})\}$*

Theorem 1.3.3 (Equivalence of symmetric subspace and unitary tensor span)**.** *Let $\mathcal{X}$ be a complex Euclidean space and k be a positive integer. Then the symmetric subspace of linear operators is equivalent to the span of the unitary tensor products, i.e.,*

$$\mathcal{L}(\mathcal{X})^{\otimes k} = Span\{U^{\otimes k} : U \in \mathcal{U}(\mathcal{X})\}. \tag{1.14}$$

Lemma 1.3.4 (Invariant subspace lemma)**.** *Let $\mathcal{X}$ be a complex Euclidean space, let $\mathcal{V} \subseteq \mathcal{X}$ be a subspace, and let $A \in \mathcal{L}(\mathcal{X})$ be an operator. The following statements are equivalent:*

1. *It holds that both $A\mathcal{V} \subseteq \mathcal{V}$ and $A^*\mathcal{V} \subseteq \mathcal{V}$.*
2. *It holds that $[A, \Pi_{\mathcal{V}}] = 0$.*

Theorem 1.3.5 (Double Commutant Theorem)**.** *Let $\mathcal{A}$ be a self-adjoint, unital subalgebra of $\mathcal{L}(\mathcal{X})$. Then the double commutant of $\mathcal{A}$ is equal to $\mathcal{A}$, i.e.,*

$$Comm(Comm(\mathcal{A})) = \mathcal{A}. \tag{1.15}$$

Proof. For all $X \in \text{Comm}(\mathcal{A})$ and any $A \in \mathcal{A}$, we have

$$[X, A] = AX - XA = 0. \tag{1.16}$$

Therefore, $A \in \text{Comm}(\text{Comm}(\mathcal{A}))$, so $\mathcal{A} \subseteq \text{Comm}(\text{Comm}(\mathcal{A}))$.

To demonstrate reverse inclusion, consider the subalgebra $\mathcal{B} \subseteq \mathcal{L}(\mathcal{X} \otimes \mathcal{X})$ defined as

$$\mathcal{B} = \{X \otimes \mathbb{I} : X \in \mathcal{A}\}. \tag{1.17}$$

For all $Y \in \mathcal{L}(\mathcal{X} \otimes \mathcal{X})$, it can be written in terms of the standard computational basis

$$Y = \sum_{i,j \in [d]} \sum_{a,b \in [d]} c_{i,j,a,b} |i\rangle\langle j| \otimes |a\rangle\langle b|. \tag{1.18}$$

Using the definition of the standard computational basis of operators, we can rearrange the right-hand side into the form

$$Y = \sum_{a,b \in [d]} Y_{a,b} \otimes E_{a,b} \tag{1.19}$$

where $Y_{a,b} = \sum_{i,j \in [d]} c_{i,j,a,b} |i\rangle\langle j|$.

Y commutes with $\mathcal{B}$ if and only if $Y(X \otimes \mathbb{I}) = (X \otimes \mathbb{I})Y$ for all $X \in \mathcal{A}$. Substituting Equation 1.19 and simplifying shows that Y commutes with $\mathcal{B}$ if and only if $[Y_{a,b}, X] = 0$. For any $X \in \text{Comm}(\text{Comm}(\mathcal{A}))$, X must commute with $\text{Comm}(\mathcal{A})$, and therefore

$$X \otimes \mathbb{I} \in \text{Comm}(\text{Comm}(\mathcal{B})). \tag{1.20}$$

It remains to show that every element in Comm(Comm($\mathcal{B}$)) is of the form $X \otimes \mathbb{I}$. Define a subspace $\mathcal{V} \subseteq X \otimes X$, where

$$\mathcal{V} = \left\{ \mathrm{vec}(X) = \sum_{a,b\in[d]} c_{a,b}|a\rangle \otimes |b\rangle : X \in \mathcal{A} \right\}. \tag{1.21}$$

For any arbitrary $X \in \mathcal{A}$, we find that

$$\begin{aligned}
(X \otimes \mathbb{I})\mathcal{V} &= \{(X \otimes \mathbb{I})V : V \in \mathcal{V}\} \\
&= \left\{ (X \otimes \mathbb{I}) \left(\sum_{a,b\in[d]} c_{a,b}|a\rangle \otimes |b\rangle \right) : \sum_{a,b\in[d]} c_{a,b}|a\rangle\langle b| \in \mathcal{A} \right\} \\
&= \left\{ \sum_{a,b\in[d]} c_{a,b}X|a\rangle \otimes |b\rangle : \sum_{a,b\in[d]} c_{a,b}|a\rangle\langle b| \in \mathcal{A} \right\} \\
&\subseteq \mathcal{V},
\end{aligned} \tag{1.22}$$

the inclusion of which follows from the fact that $\mathcal{A}$ is an algebra so $X|a\rangle = Xe_a \in \mathcal{A}$. Similarly, since $\mathcal{A}$ is self-adjoint,

$$(X^* \otimes \mathbb{I})\mathcal{V} \subseteq \mathcal{V}. \tag{1.23}$$

By Lemma 1.3.4, this implies $[X \otimes \mathbb{I}, \Pi_{\mathcal{V}}] = 0$, and hence

$$\Pi_{\mathcal{V}} \in \mathrm{Comm}(\mathcal{B}). \tag{1.24}$$

Therefore, for any arbitrary $X \in \mathrm{Comm}(\mathrm{Comm}(\mathcal{A}))$, Equation 1.20 implies

$$X \otimes \mathbb{I} \in \mathrm{Comm}(\mathrm{Comm}(\mathcal{B})). \tag{1.25}$$

It follows from Equation 1.24 that

$$[X \otimes \mathbb{I}, \Pi_{\mathcal{V}}] = 0. \tag{1.26}$$

By Lemma 1.3.4, this yields

$$(X \otimes \mathbb{I})\mathcal{V} \subseteq \mathcal{V}. \tag{1.27}$$

Since the subalgebra $\mathcal{A}$ is unital, $\mathbb{I} \in \mathcal{A}$ and thus $\mathrm{vec}(\mathbb{I}) \in \mathcal{V}$. Therefore,

$$\begin{aligned}
(X \otimes \mathbb{I})\mathrm{vec}(\mathbb{I}) &= (X \otimes \mathbb{I}) \sum_{a\in[d]} |a\rangle \otimes |a\rangle \\
&= \sum_{a\in[d]} X|a\rangle \otimes |a\rangle = \sum_{a\in[d]} \left(\sum_{b,c\in[d]} X_{b,c}|b\rangle\langle c| \right) |a\rangle \otimes |a\rangle \\
&= \sum_{a\in[d]} \sum_{b\in[d]} X_{b,a}|b\rangle \otimes |a\rangle \\
&= \sum_{b,a\in[d]} X_{b,a}|b\rangle \otimes |a\rangle = \mathrm{vec}(X) \in \mathcal{V}.
\end{aligned} \tag{1.28}$$

By the bijectivity of vec, $X \in \mathcal{A}$, so $\mathrm{Comm}(\mathrm{Comm}(\mathcal{A})) \subseteq \mathcal{A}$. □

Theorem 1.3.6 (Schur-Weyl duality). *Let $\mathcal{X}$ be a complex Euclidean space, k be a positive integer, and $X \in \mathcal{L}(\mathcal{X}^{\otimes k})$ be an operator. Then the set of all commutators of the unitary group is equivalent to the span of the permutation operators, i.e.,*

$$\mathit{Comm}(\mathcal{U}(\mathcal{X}), k) = \mathit{Span}\{W_\pi : \pi \in S_k\} \tag{1.29}$$

Proof. Let $X \in \mathrm{Comm}(\mathcal{U}(\mathcal{X}), k)$. then by the bilinearity of the Lie bracket,

$$X \in \mathrm{Comm}(\mathrm{Span}\{U^{\otimes k} : U \in U(\mathcal{X})\}) \tag{1.30}$$

Proposition 1.3.2 implies that $X \in \mathrm{Comm}(\mathcal{L}(\mathcal{X})^{\oslash k})$, so

$$\mathrm{Comm}(\mathrm{Span}\{U^{\otimes k} : U \in U(\mathcal{X})\}) = \mathrm{Comm}(\mathcal{L}(\mathcal{X})^{\oslash k}). \tag{1.31}$$

By Definition 1.2.1, $Z \in \mathcal{L}(\mathcal{X})^{\oslash}$ if and only if there exists some $X \in \mathcal{L}(\mathcal{X})$ such that

$$Z = X = W_\pi X W_\pi^* \text{ for all } \pi \in S_k. \tag{1.32}$$

Right-multiplying and rearranging by W_π yields $XW_\pi - W_\pi X = 0$, and so by the bilinearity of the Lie bracket,

$$Z = X \in \mathrm{Comm}(\mathrm{Span}\{W_\pi : \pi \in S_k\}). \tag{1.33}$$

Hence

$$\mathcal{L}(\mathcal{X})^{\oslash k} = \mathrm{Comm}(\mathrm{Span}\{W_\pi : \pi \in S_k\}). \tag{1.34}$$

By Theorem 1.3.5, taking the commutant of both sides yields

$$\mathrm{Comm}(\mathcal{L}(\mathcal{X})^{\oslash k}) = \mathrm{Span}\{W_\pi : \pi \in S_k\}. \tag{1.35}$$

By substitution of Eq. 1.31, we have shown

$$\mathrm{Comm}(U(\mathcal{X}), k) = \mathrm{Span}\{W_\pi : \pi \in S_k\}. \tag{1.36}$$

□

1.4 Examples

1.4.1 Group Averaging and Pauli Twirling

We illustrate some simple examples of Haar measure computations. In particular, we are interested in first-order computations on discrete and continuous groups. We approach this from the perspective of group averaging and twirling.

Definition 1.4.1 (Group average)**.** Let G be a group of order N and R a representation of the group. Define the group average to be

$$\langle X \rangle_G = \frac{1}{N} \sum_g R(g) X R(g)^\dagger. \tag{1.37}$$

Remark 1.4.2 (Assumptions). Consider a n-qubit system. Let $d = 2^n$, and suppose we seek to compute moments of order k. We assume for now that $d > k$ for the examples below.

1.4.2 Pauli twirling

The end goal of this section is to prove the Irrep Group Averaging Corollary

$$\langle X \rangle_G = \frac{1}{d} \mathrm{Tr}[X] I, \tag{1.38}$$

where $n_a = d$ is the dimension of the vector space of the representation. To illustrate this, we first consider the group average of the single-qubit Pauli group on some arbitrary initial state ρ.

Remark 1.4.3 (Pauli groups). We denote the single-qubit Pauli group as

$$G = \{\pm(i)\sigma_x, \pm(i)\sigma_y, \pm(i)\sigma_z, \pm(i)I\}, \tag{1.39}$$

where the Pauli matrices are given by

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.40}$$

We note the following useful expressions.

Definition 1.4.4 (Bloch vectors)**.** For any single-qubit quantum state ρ, we can write it in terms of its Bloch vector,

$$\rho = \frac{1}{2}(I + r \cdot \sigma), \tag{1.41}$$

where $r = (r_x, r_y, r_z) \in \mathbb{R}^3$ is the coordinate of the quantum state on the Bloch sphere and $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ is a three-tuple of the Pauli operators.

Remark 1.4.5 (Pauli group identities). For all non-identity σ_i, σ_j in the Pauli group where $i \neq j$, the following three statements are true.

1. $\sigma_i \sigma_j \sigma_i = -\sigma_j$,
2. $\sigma_j^3 = \sigma_j$, and
3. $\sigma_i^2 = \sigma_i$, since σ_i is represented by a self-adjoint matrix.

We want to show the following simpler equivalence using matrix computations.

Theorem 1.4.6 (Pauli twirling of a single qubit)**.** *For an arbitrary single-qubit state ρ,*

$$\langle \rho \rangle_G = \frac{1}{N} \sum_g R(g) X R(g)^\dagger = \frac{I}{2}, \tag{1.42}$$

the maximally mixed state (since it is proportional to the identity matrix).

Proof. Note that G has order $N = 4$. For any Pauli operator $\pm(i)X \in G$, X is self-adjoint. Thus, we have that

$$\pm(i)X\rho(\pm(i)X)^\dagger = (\pm i)(\mp i)X\rho X = X\rho X. \tag{1.43}$$

By Def. 1.4.1 and Eq. 1.43,

$$\langle \rho \rangle_G = \frac{1}{4}\left(\sigma_x \rho \sigma_x + \sigma_y \rho \sigma_y + \sigma_z \rho \sigma_z + I \rho I\right). \tag{1.44}$$

By Remark 1.4.4 and Remark 1.4.5, we can rewrite ρ such that

$$\begin{aligned}
\langle \rho \rangle_G &= \frac{1}{4}\left(\sigma_x(\frac{1}{2}(I + r\cdot\sigma)\sigma_x + \sigma_y(\frac{1}{2}(I + r\cdot\sigma))\sigma_y + \sigma_z(\frac{1}{2}(I + r\cdot\sigma))\sigma_z + I(\frac{1}{2}(I + r\cdot\sigma))I\right) \\
&= \frac{1}{4}\left(\frac{1}{2}\left[\sigma_x I \sigma_x + r_x\sigma_x^3 + r_y\sigma_x\sigma_y\sigma_x + r_z\sigma_x\sigma_z\sigma_x\right] + \frac{1}{2}\left[\sigma_y I\sigma_y + r_x\sigma_y\sigma_x\sigma_y + r_y\sigma_y^3 + r_z\sigma_y\sigma_z\sigma_y\right]\right. \\
&\quad \left. + \frac{1}{2}\left[\sigma_z I\sigma_z + r_x\sigma_z\sigma_x\sigma_z + r_y\sigma_z\sigma_y\sigma_z + r_z\sigma_z^3\right] + \frac{1}{2}\left[I^3 + r_x I\sigma_x I + r_y I\sigma_y I + r_z I\sigma_z I\right]\ \right) \\
&= \frac{1}{8}\left(\ [I + r_x\sigma_x - r_y\sigma_y - r_z\sigma_z] + [I - r_x\sigma_x + r_y\sigma_y - r_z\sigma_z]\right. \\
&\quad \left. + [I - r_x\sigma_x - r_y\sigma_y + r_z\sigma_z] + [I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z]\ \right) \\
&= \frac{1}{8}(4I) = \frac{I}{2}.
\end{aligned} \tag{1.45}$$

□

1.4.3 Explicit Calculation of single qubit first moment

We consider systems of n qubits, represented by vectors of dimension $d = 2^n$. Consider the calculation of the first moment of a system with $n = 1$. Due to the small size of the system, we can explicitly define the Haar measure and parameterize the unitary in our calculations, which we do in the example below.

Remark 1.4.7 (Explicit construction of 2×2 unitaries). Every unitary U in the unitary group of size 2×2, denoted $U(2)$, can be parameterized in terms of $\phi, \theta, \omega \in \mathbb{R}$, where

$$U = \begin{bmatrix} e^{-i(\phi+\omega)/2} \cos \frac{\theta}{2} & -e^{i(\phi-\omega)/2} \sin \frac{\theta}{2} \\ e^{-i(\phi-\omega)/2} \sin \frac{\theta}{2} & e^{i(\phi+\omega)/2} \cos \frac{\theta}{2} \end{bmatrix}. \tag{1.46}$$

The conjugate transpose $U^\dagger$ is given by

$$U^\dagger = \begin{bmatrix} e^{i(\phi+\omega)/2} \cos \frac{\theta}{2} & e^{i(\phi-\omega)/2} \sin \frac{\theta}{2} \\ -e^{-i(\phi-\omega)/2} \sin \frac{\theta}{2} & e^{-i(\phi+\omega)/2} \cos \frac{\theta}{2} \end{bmatrix}. \tag{1.47}$$

Let μ_H denote the generalized Haar measure on any n-qubit system. On a single qubit, we can write the moment calculation in terms of the expectation value, which in turn can be written as an integral under μ_H. The first moment of the operator of an n-qubit system O, where $O \in \mathcal{L}(\mathbb{C}^d)$, is

$$\mathbb{E}_{U\sim\mu_H}[UOU^\dagger] = \int_{U\sim\mu_H} UOU^\dagger d\mu_H. \tag{1.48}$$

We now define a Haar measure specific to the case $n = 1$.

Definition 1.4.8 (Parameterized single-qubit Haar measure)**.** Let μ_2 denote the Haar measure on a single qubit, represented with vectors in $\mathbb{C}^2$. Define the single-qubit Haar measure in terms of the parameters given in Remark 1.4.7, where

$$d\mu_2 = \sin\theta d\theta \cdot d\omega \cdot d\phi \tag{1.49}$$

is the unnormalized Haar measure. The normalized computation of moments using the Haar measure is given by

$$\mathbb{E}_{U\sim\mu_2}[UOU^\dagger] = \frac{1}{8\pi^2} \int_{\phi=0}^{2\pi} \int_{\omega=0}^{2\pi} \int_{\theta=0}^{\pi} UOU^\dagger \sin\theta d\theta d\omega d\phi, \tag{1.50}$$

where the factor of $\frac{1}{8\pi^2}$ can be found by computing the integral and setting $UOU^\dagger = 1$.

Remark 1.4.9 (Reordering parameters). We may reorder the parameters ϕ, ω, and θ in the integral by Fubini's theorem. An alternative way to state the normalized computation of moments using the Haar measure is

$$\mathbb{E}_{U\sim\mu_2}[UOU^\dagger] = \frac{1}{8\pi^2} \int_{\theta=0}^{\pi} \int_{\phi=0}^{2\pi} \int_{\omega=0}^{2\pi} UOU^\dagger \sin\theta d\omega d\phi d\theta. \tag{1.51}$$

We can keep the boundaries of the parameters the same, as they are independent of the order of integration.

Theorem 1.4.10 (Example: First moment of Pauli-Z operator)**.** *Consider $O = \sigma_z$, the Pauli-Z operator. We show that*

$$\mathbb{E}_{U\sim\mu_2}[U\sigma_z U^\dagger] = \frac{Tr(\sigma_z)}{2} I. \tag{1.52}$$

Proof. The Pauli-Z operator is given by

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.53}$$

Hence

$$\frac{\mathrm{Tr}(\sigma_z)}{2} I = \frac{0}{2} I = \mathbf{0}, \tag{1.54}$$

where $\mathbf{0}$ is the zero matrix. Given Def. 1.4.8, we seek to show that

$$\mathbb{E}_{U\sim\mu_2}[U\sigma_z U^\dagger] = \frac{1}{8\pi^2}\int_{\phi=0}^{2\pi}\int_{\omega=0}^{2\pi}\int_{\theta=0}^{\pi} UOU^\dagger \sin\theta d\theta d\omega d\phi \tag{1.55}$$

is equivalent. We explicitly compute the inner matrix multiplication:

$$\begin{aligned} U\sigma_z U^\dagger &= \begin{bmatrix} e^{-i(\phi+\omega)/2}\cos\frac{\theta}{2} & -e^{i(\phi-\omega)/2}\sin\frac{\theta}{2} \\ e^{-i(\phi-\omega)/2}\sin\frac{\theta}{2} & e^{i(\phi+\omega)/2}\cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} e^{i(\phi+\omega)/2}\cos\frac{\theta}{2} & e^{i(\phi-\omega)/2}\sin\frac{\theta}{2} \\ -e^{-i(\phi-\omega)/2}\sin\frac{\theta}{2} & e^{-i(\phi+\omega)/2}\cos\frac{\theta}{2} \end{bmatrix} \\ &= \begin{bmatrix} \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} & e^{-i\omega}\cos\frac{\theta}{2}\sin\frac{\theta}{2} + e^{-i\omega}\sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ e^{i\omega}\sin\frac{\theta}{2}\cos\frac{\theta}{2} + e^{i\omega}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} - \cos^2\frac{\theta}{2} \end{bmatrix} \end{aligned} \tag{1.56}$$

Evaluating the integral for either ϕ or ω in the interval $[0, 2\pi)$ gives

$$\int_{\phi=0}^{2\pi} e^{ic_\phi\phi} d\phi = 0 \qquad \text{and} \qquad \int_{\omega=0}^{2\pi} e^{ic_\omega\omega} d\omega = 0. \tag{1.57}$$

Consequently, in the expanded form of $UOU^\dagger$, any elements with a remaining dependence (i.e., a nonzero c_ϕ or c_ω) on either ϕ or ω will integrate to zero. Consequently, we find

$$\begin{aligned} &\frac{1}{8\pi^2}\int_{\theta=0}^{\pi}\int_{\phi=0}^{2\pi}\int_{\omega=0}^{2\pi} \begin{bmatrix} \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} & e^{-i\omega}\cos\frac{\theta}{2}\sin\frac{\theta}{2} + e^{-i\omega}\sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ e^{i\omega}\sin\frac{\theta}{2}\cos\frac{\theta}{2} + e^{i\omega}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} - \cos^2\frac{\theta}{2} \end{bmatrix} \sin\theta d\omega d\phi d\theta \\ &= \frac{1}{8\pi^2}\int_{\theta=0}^{\pi} 4\pi^2 \begin{bmatrix} \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} & 0 \\ 0 & \sin^2\frac{\theta}{2} - \cos^2\frac{\theta}{2} \end{bmatrix} \sin\theta d\theta \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{0}. \end{aligned} \tag{1.58}$$

□

1.4.4 Commutant of the First Order Unitary Group

Applying Schur's lemma

Remark 1.4.11 (Schur's Lemma). For a finite-dimensional complex representation V of a group G that is irreducible under the action of $\mathcal{U}(2)$, every G-equivariant endomorphism of V (i.e., a linear map from $V \to V$) is a scalar multiple of the identity.

Proposition 1.4.12. *Let $v, w \in \mathbb{C}^2$ be unit vectors (i.e., $|v| = |w| = 1$). Then there exists a unitary matrix $U \in U(2)$ such that $Uv = w$.*

Proof. Let $S = \{z \in \mathbb{C}^2 : |z| = 1\}$ denote the unit sphere under $\mathbb{C}^2$, which is acted upon by $\mathcal{U}(2)$ through matrix multiplication. Since the action of $\mathcal{U}(2)$ preserves the Hermitian inner product, for any $U \in \mathcal{U}(2)$ and vector $z \in \mathbb{C}^2$, we have that

$$|Uz|^2 = |z|^2. \tag{1.59}$$

So the action of U is a well-defined action over the set S.

We seek to show that the action of any U in $\mathcal{U}(2)$ on S is transitive. Equivalently, we seek to show that for any $v, w \in S$, the orbit of v contains w. Let e_1 be the standard basis vector in S, where e_1 is given by

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{1.60}$$

Let $x \in S^3$ be an arbitrary unit vector. We can extend the singleton set $\{x\}$ to an orthonormal basis $\mathcal{B}_x = \{x, x^\perp\}$ of $\mathbb{C}^2$. Similarly, let $\mathcal{B}_{e_1} = \{e_1, e_2\}$ be the standard orthonormal basis.

Define a linear operator $T : \mathbb{C}^2 \to \mathbb{C}^2$ by specifying its action on the basis $\mathcal{B}_{e_1}$:

$$T(e_1) = x \quad \text{and} \quad T(e_2) = x^\perp. \tag{1.61}$$

Since T maps an orthonormal basis to an orthonormal basis, it preserves inner products. Specifically, for any $u, v \in \mathbb{C}^2$, $\langle Tu, Tv\rangle = \langle u, v\rangle$. A linear operator on a finite-dimensional inner product space that preserves the inner product is unitary. Thus, $T \in U(2)$. By construction, $Te_1 = x$.

Since x was arbitrary, the orbit of e_1 is S^3. Now, let $v, w \in S^3$ be the given vectors. By the transitivity established above, there exist matrices $U_1, U_2 \in U(2)$ such that:

$$U_1 e_1 = v \quad \text{and} \quad U_2 e_1 = w. \tag{1.62}$$

Since $U(2)$ is a group, U_1^{-1} exists and is unitary. Define $U = U_2 U_1^{-1}$. Then $U \in U(2)$, and:

$$Uv = (U_2 U_1^{-1})v = U_2(U_1^{-1}v) = U_2 e_1 = w. \tag{1.63}$$

Thus, there exists a unitary matrix U such that $Uv = w$. □

Theorem 1.4.13 (Commutant of first order unitaries is a scalar multiple of the identity)**.** *Given the identity* $\mathbb{I} \in \mathcal{U}(2)$*,*

$$\{M : MU = UM, \forall U \in \mathcal{U}(2)\} = \{\lambda\mathbb{I} : \lambda \in \mathbb{C}\}. \tag{1.64}$$

Proof. We first show forward inclusion, where $\{M : MU = UM, \forall U \in \mathcal{U}(2)\} \subseteq \{\lambda\mathbb{I} : \lambda \in \mathbb{C}\}$. Let $V = \mathbb{C}^2$ be the complex vector space of dimension 2 acted upon by $\mathcal{U}(2)$. We show that V is irreducible.

Clearly $\{0\}$ is a subspace of V. Suppose $W \subseteq V$ is a nonzero $\mathcal{U}(2)$-invariant subspace. Note that the natural action of $\mathcal{U}(2)$ is transitive on the unit sphere of $\mathbb{C}^2$, as given in Lemma 1.4.12. Since V has dimension 2 by definition, $\dim(W) = 1$ or $\dim(W) = 2$. Assume for contradiction that $\dim(W) = 1$, and let $v \in W$ be a unit vector. By transitivity, $\mathcal{U}(2)v$ covers the entire unit sphere of V. That is, for all $w \in W$, there exists a U such that $Uv = w$. Since W is $\mathcal{U}(2)$-invariant, W must contain the entire unit sphere and therefore spans V, implying $\dim(W) = 2$. So $V = W$. Since the only subspaces of V are the zero subspace and itself, V is irreducible. Note that $MU = UM$ implies M is a $\mathcal{U}(2)$-equivariant endomorphism of V. By Schur's lemma, as restated in Remark 1.4.11

$$M = \lambda\mathbb{I}, \tag{1.65}$$

where $\lambda \in \mathbb{C}$.

Conversely, it is trivial that any scalar multiple of the identity commutes with all $U \in \mathcal{U}(2)$. □

Applying the Schur-Weyl duality

We now write an outline based on the Schur-Weyl duality.

Lemma 1.4.14 (Span of 1D permutations is the span of $\mathbb{I}$)**.** *Let $d \in \mathbb{N}$ and $k = 1$. Then*

$$Span\{V_d(\pi) : \pi \in S_k\} = Span(\mathbb{I}). \tag{1.66}$$

Proof. In a tensor product composed of one element, any permutation of the tensor product simply returns the element itself. □

Theorem 1.4.15 (Using Schur-Weyl Duality for Commutants)**.** *Given the identity $\mathbb{I} \in \mathcal{U}(2)$,*

$$\{M : MU = UM, \forall U \in \mathcal{U}(2)\} = \{\lambda\mathbb{I} : \lambda \in \mathbb{C}\}. \tag{1.67}$$

We prove this statement now using the abstract Schur-Weyl duality.

Proof. Observe that the left-hand side can be equivalently written as

$$\{M : MU = UM, \forall U \in \mathcal{U}(2)\} = \{M : MU^{\otimes 1} = U^{\otimes 1}M, \forall U \in \mathcal{U}(2)\}. \tag{1.68}$$

By the Schur-Weyl duality and transitivity of equality,

$$\{M : MU = UM, \forall U \in \mathcal{U}(2)\} = \text{Span}(\mathbb{I}) = \{\lambda\mathbb{I} : \lambda \in \mathbb{C}\} \tag{1.69}$$

□

Generalized Commutant of kth Order Unitary Group

Theorem 1.4.16. *Consider the set of $\mathcal{U}(2)^{\otimes k}$ defined over $\mathbb{C}$. We show that*

$$\{M : MU^{\otimes k} = U^{\otimes k}M, \forall U \in \mathcal{U}(2)\} = Span\{V_d(\pi) : \pi \in S_2\}. \tag{1.70}$$