(Introduction to Haar measure tools in Quantum Information — Antonio Anna Mele) $\boxed{B}$

Story: We now prove special case of Schur-Weyl duality, i.e. for $k=1$ & 2, we show that

$$\mathrm{Comm}(\mathbb{U}(d), k) = \mathrm{span}\{V_d(\pi) : \pi \in S_k\}$$

Example 14.

(i) $\mathrm{Comm}(\mathbb{U}(d), k=1) = \mathrm{span}\{I\}$

(ii) $\mathrm{Comm}(\mathbb{U}(d), k=1) = \mathrm{span}\{\mathbb{1}, \mathbb{F}\}$

Proof (i) Consider an element $A \in \mathrm{Comm}(\mathbb{U}(d), k=1)$.

NB: In the canonical basis, one can write

$$A = \sum_{i,j=1}^{d} A_{ij}\, |i\rangle\langle j|$$
$$= \sum_{i=1}^{d} A_{ii}\, |i\rangle\langle i| + \sum_{\substack{i,j=1 \\ i\neq j}}^{d} A_{ij}\, |i\rangle\langle j|$$

where $A_{ij} := \langle i|A|j\rangle$

NB2: $UAU^{+} = A \quad \forall\, U \quad \because \quad A \in \mathrm{Comm}(\mathbb{U}(d), k=1)$.

Consider: $U_k := \sum_{i\neq k} |i\rangle\langle i| - |k\rangle\langle k|$

i.e. it maps $|k\rangle$ to $-|k\rangle$.

NB: $U_k\, A\, U_k^{+} = A$

$\Rightarrow \quad A_{kl}\, |k\rangle\langle l| = -A_{kl}\, |k\rangle\langle l| \quad \forall\, l\neq k$.

$\Rightarrow \quad A_{kl} = 0, \quad \forall\, l\neq k$.

This is true for any arbitrary k.

NB2: $\Rightarrow A = \sum_{i=1}^{d} A_{ii}\, |i\rangle\langle i|$

Consider: $U_{k\ell} := \sum_{i \notin \{k,\ell\}} |i\rangle\langle i| + |k\rangle\langle \ell| + |\ell\rangle\langle k|$

i.e. $U_{k\ell}$ sends $|k\rangle$ to $|\ell\rangle$ & $|\ell\rangle$ to $|k\rangle$

but leaves every other vector unchanged.

NB: $U_{k\ell} A U_{k\ell}^\dagger = A$

$\Rightarrow \quad A_{kk} = A_{\ell\ell}$

Conclusion: $A = c \sum_{i=1}^{d} |i\rangle\langle i| = c I$, as asserted in (i)

(ii) Consider: $Q \in \mathrm{Comm}(\mathbb{U}(d), k=2)$.

NB: Q can be decomposed as

$$Q = \sum_{ijk\ell=1}^{d} Q_{ijk\ell} |ij\rangle\langle k\ell|$$

where $Q_{ijk\ell} := \langle ij| Q |k\ell\rangle$.

NB2: $U^{\otimes 2} A U^{\dagger\otimes 2} = A \quad \forall\ U \in \mathbb{U}(d)$

Consider: $U_{k'} := \sum_{i \neq k'} |i\rangle\langle i| - |k'\rangle\langle k'|$

(i.e., as before, sends a basis vector to its negative, leaving others unchanged).

NB3: $\forall\ i,j,k,\ell \in [d]$ s.t. $\{i,j\} \neq \{k,\ell\}$

it holds that $Q_{ij;k\ell} |ij\rangle\langle k\ell| = -Q_{ij;k\ell} |ij\rangle\langle k\ell|$

$(\Leftarrow \quad U_{k'} Q U_{k'}^\dagger = Q$ for some k')

NB4: Thus, Q has the following form

$$Q = \sum_{i=1}^{d} Q_{i,i;i,i} \, |ii\rangle\langle ii| + \sum_{i\neq j} Q_{ij;ij} \, |ij\rangle\langle ij| + \sum_{i\neq j} Q_{ij;ji} \, |ij\rangle\langle ji|$$

($\because$ $\{i,j\} = \{k,l\}$ i.e., either $i=k$, $j=l$ or $i=l$, $j=k$ or $i=j=k=l$)

Consider: $U_{ij\to kl} := \sum_{i'j' \neq \{ij,kl\}} |i'j'\rangle\langle i'j'| + \left(|ij\rangle\langle kl| + h.c.\right)$

NB: Using $U^{\otimes 2} Q U^{\dagger\otimes 2} = Q$, for $U_{ij\to kl}$,
it follows that

$$Q = \underbrace{a}_{=Q_{11;11}} \sum_{i=1}^{d} |ii\rangle\langle ii| + \underbrace{b}_{=Q_{12;12}} \sum_{i\neq j} |ij\rangle\langle ij| + \underbrace{c}_{=Q_{12;21}} \sum_{i\neq j} |ij\rangle\langle ji|$$

NB2: $$Q = (a-b-c)\sum_{i=1}^{d} |ii\rangle\langle ii| + b\mathbb{1} + c\mathbb{F}$$

NB3: $\because$ $\mathbb{1}, \mathbb{F} \in \mathrm{Comm}(\mathbb{U}(d),2)$,
$Q \in \mathrm{Comm}(\mathbb{U}(d),2)$ iff $\sum_{i=1}^{d} |ii\rangle\langle ii| \in \mathrm{Comm}(\mathbb{U}(d),2)$.

claim: $\sum_{i=1}^{d} |ii\rangle\langle ii| \notin \mathrm{Comm}(\mathbb{U}(d),2)$
(proved below)

NB4: Thus, $Q = b\mathbb{1} + c\mathbb{F} \in \mathrm{span}\{\mathbb{1}, \mathbb{F}\}$ as asserted.

Proof of the claim
Suppose: $\sum_i |ii\rangle\langle ii| \in \mathrm{Comm}(\mathbb{U}(d),2)$.
(for contradiction)

Consider: $U_{DFT} = \frac{1}{\sqrt{d}} \sum_{jk} \omega^{(j-1)(k-1)} |j\rangle\langle k|$

where $\omega := e^{\frac{i2\pi}{d}}$

Then: $U_{DFT}^{\otimes 2} \left(\sum_i |ii\rangle\langle ii|\right) U_{DFT}^{\dagger\otimes 2} = \sum_i |ii\rangle\langle ii|$

$$\Rightarrow \quad \langle 11| U_{DFT}^{\otimes 2} \left(\sum_i |ii\rangle\langle ii|\right) U_{DFT}^{\otimes 2} |11\rangle = 1$$

$\parallel$ calculation

contradiction

$$\frac{1}{d}$$

$$\left(\frac{1}{d} \sum_{kk'} w^0 \langle k\, k'| \left(\sum_i |ii\rangle\langle ii|\right) \sum_{k''k'''} w^0 |k''k'''\rangle \frac{1}{d} \right.$$

$$\left. = \frac{1}{d^2} \sum_i = \frac{d}{d^2} = \frac{1}{d} \right)$$

$\square$

$\square$

§ 4. Symmetric Subspace

Story:
- We introduce the symmetric subspace
  - it plays a crucial role when analysing Haar random states
  - in-depth analysis is deferred to [61].
- The symmetric subspace can be defined as the set of states $|\psi\rangle$ in $(\mathbb{C}^d)^{\otimes k}$ that are invariant under the permutations of their constituent subsystems.

Def^n 15 (Symmetric Subspace)

$$\mathrm{Sym}_k(\mathbb{C}^d) := \{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes k} : V_d(\pi)|\psi\rangle = |\psi\rangle \ \forall \pi \in S_k \}.$$

Story: It helps to define the following.

Not^n: $$P_{sym}^{(d,k)} := \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi).$$

Theorem 16 (Projection on $Sym_k(\mathbb{C}^d)$).

$P^{(d,k)}$ is the orthogonal projector on the symmetric subspace $Sym_k(\mathbb{C}^d)$.

Proof

NB1: $V_d(\pi)\, P_{sym}^{(d,k)} = P_{sym}^{(d,k)}$

$$\left(\because \quad V_d(\pi)\, P_{sym}^{(d,k)} = \frac{1}{k!} \sum_{\sigma \in S_k} V_d(\pi)\, V_d(\sigma) = \frac{1}{k!} \sum_{\sigma \in S_k} V_d(\pi\sigma) = \frac{1}{k!} \sum_{\sigma \in S_k} V_d(\sigma) = P_{sym}^{(d,k)}. \right)$$

NB2: $\left(P_{sym}^{(d,k)}\right)^2 = P_{sym}^{(d,k)}$

$$\left(\because \quad \left(P_{sym}^{(d,k)}\right)^2 = \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi)\, P_{sym}^{(d,k)} = \frac{1}{k!} \sum_{\pi \in S_k} P_{sym}^{(d,k)} \quad \text{(using NB)} \quad = P_{sym}^{(d,k)} \right)$$

NB3: $\left(P_{sym}^{(d,k)}\right)^\dagger = P_{sym}^{(d,k)}$

$$\left(\because \quad \left(P_{sym}^{(d,k)}\right)^\dagger = \frac{1}{k!} \sum_{\pi \in S_k} V_d^\dagger(\pi) = \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi^{-1}) = \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi) = P_{sym}^{(d,k)} \right)$$

Conclusion: $P^{(d,k)}_{sym}$ is an orthogonal projector

Strategy: We now show that

$$\text{(i) } \mathrm{Im}(P^{(d,k)}_{sym}) \subseteq \mathrm{Sym}_k(\mathbb{C}^d) \text{ \& }$$

$$\text{(ii) } \mathrm{Sym}_k(\mathbb{C}^d) \subseteq \mathrm{Im}(P^{(d,k)}_{sym})$$

which establish the theorem.

Proof of (i):

NB4: $P^{(d,k)}_{sym} |\psi\rangle \in \mathrm{Sym}_k(\mathbb{C}^d) \quad \forall\, |\psi\rangle$

$\because \quad V_d(\pi)\, P^{(d,k)}_{sym} |\psi\rangle = P^{(d,k)}_{sym} |\psi\rangle$

(from NB1)

i.e. $V_d(\pi) P^{(d,k)}_{sym} = P^{(d,k)}_{sym}$

(ii)

NB5: $\forall \; |\psi\rangle \in \mathrm{Sym}_k(\mathbb{C}^d)$,

$$P^{(d,k)}_{sym} |\psi\rangle = \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi) |\psi\rangle$$

$$= \frac{1}{k!} \sum_{\pi \in S_k} |\psi\rangle = |\psi\rangle$$

$\square$

Theorem 17 (Dimension of the symmetric subspace).

$$\mathrm{tr}\left(P^{(d,k)}_{sym}\right) = \dim\left(\mathrm{Sym}_k(\mathbb{C}^d)\right) = \binom{k+d-1}{k}$$

Proof:

NB: The first equality holds because $P^{(d,k)}_{sym}$ is an orthogonal projector onto $\mathrm{Sym}_k(\mathbb{C}^d)$.

NB2: $\mathrm{Sym}_k(\mathbb{C}^d) = \mathrm{Im}(P^{(d,k)}_{sym})$ (thm 16)

$= \mathrm{span}\{P^{(d,k)}_{sym}|i_1 \dots i_k\rangle : i_1 \dots i_k \in [d]\}$.

goal: To count the # of independent vectors in this set.

suppose: $|i_1 \dots i_k\rangle$ &

$|j_1 \dots j_k\rangle$ are s.t.

$\{i_1 \dots i_k\}$ & $\{j_1 \dots j_k\}$ have

the same number n_m of

elements that are equal to m

for all $m \in [d]$.

NB: $\exists$ a unitary operator $V_d(\pi)$ s.t.

$V_d(\pi)|i_1 \dots i_k\rangle = |j_1 \dots j_k\rangle$

NB2: $\because P^{(d,k)}_{sym} V_d(\pi) = P^{(d,k)}_{sym}$, it follows that

$P^{(d,k)}_{sym}|i_1 \dots i_k\rangle = P^{(d,k)}_{sym}|j_1 \dots j_k\rangle$

Story. We therefore define vectors using $n_1, \dots n_d \in [k]$

with the constraint that they sum to k

($\because n_m$ was counting how many "systems" are

in the "state" m).

Defn: For $n_1, \dots n_d \in [k]$ with $n_1 + \dots + n_d = k$,

$|n_1 \dots n_d\rangle := P^{(d,k)}_{sym} \underbrace{|i_1\rangle \otimes \dots \otimes |i_k\rangle}$ added tensor products to emphasise the notn. remark

notn: this is not a computational basis vector

is any vector s.t. for each $m \in [d]$,

$\exists$ n_m distinct "systems" $j \in [k]$

s.t. $i_j = m$.

NB: These vectors are orthogonal & hence linearly independent.

NB2: The dim of the symmetric subspace is

then the # linearly independent vectors among

$$\{|n_1 \ldots n_d\rangle\}_{n_1+n_2 \ldots n_d = k}$$

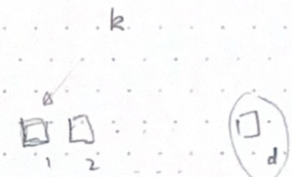
NB3: This, in turn is the number ways of assigning/distributing

k indices b/w d possible labels.

$$= \binom{k+d-1}{k}$$

me: I'm getting $\binom{k+d-1}{k-1}$

□



w.l.g. the d^{th} box's contents are fixed

$$\frac{k \cdot k-1 \ldots k-(d-1)}{d!}$$

$$\binom{n}{c} \qquad \binom{n-c}{c}$$

$$\frac{n!}{(n-c)!\,c!}$$

dist "sum" identical objects among "boxes" distinguish

$$\text{"}\binom{\text{sum} + \text{boxes} - 1}{\text{boxes} - 1}\text{"}$$

Story: We now look at the anti-symmetric subspace.

Defn 18 (Anti-symmetric subspace).

The anti-symmetric subspace is the following set:

$$\mathrm{ASym}_k(\mathbb{C}^d) := \{|\psi\rangle \in (\mathbb{C}^d)^{\otimes k} : V_d(\pi)|\psi\rangle = \mathrm{sgn}(\pi)|\psi\rangle, \ \forall\, \pi \in S_k\},$$

where $\mathrm{sgn}(\sigma)$ denotes the sign of a permutation $\sigma \in S_k$.

Story: Again, we define $P^{(d,k)}_{\mathrm{asym}}$ & prove the corresponding theorems.

Notn:
$$P^{(d,k)}_{\mathrm{asym}} := \frac{1}{k!} \sum_{\pi \in S_k} \mathrm{sgn}(\pi)\, V_d(\pi)$$

Theorem 19 The operator $P^{(d,k)}_{\mathrm{asym}}$ is the orthogonal projector on the anti-symmetric subspace $\mathrm{ASym}_k(\mathbb{C}^d)$.

⌈Proof

NB1. $V_d(\sigma) P^{(d,k)}_{asym} = \frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi) V_d(\sigma) V_d(\pi)$

$= \frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi) V_d(\sigma\pi)$

$= \frac{1}{k!} \sum_{\pi \in S_k} sgn(\sigma^{-1}\pi) V_d(\pi)$

$= sgn(\sigma^{-1}) P^{(d,k)}_{asym}$

$= sgn(\sigma) P^{(d,k)}_{asym}$

($\because$ inverse of even permutation is even & " " odd permutation is odd)

$\because$ comp even even is even
comp odd odd is even
comp even odd is odd
identity is even

NB2: One can similarly prove that
$P^{(d,k)}_{asym} V_d(\sigma) = sgn(\sigma) P^{(d,k)}_{asym}$

NB3: Using NB1 & NB2, it follows that
$\left(P^{(d,k)}_{asym}\right)^2 = P^{(d,k)}_{asym}$

$\left(\because \left(P^{(d,k)}_{asym}\right)^2 = \frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi) V_d(\pi) P^{(d,k)}_{asym} \right.$

$\left. = \frac{1}{k!} \sum_{\pi \in S_k} (sgn(\pi))^2 P^{(d,k)}_{asym} \right)$

$= P^{(d,k)}_{asym}$.

NB4: $P^{(d,k)\dagger}_{asym} = P^{(d,k)}_{asym}$

$\left(\because \left(P^{(d,k)}_{asym}\right)^\dagger = \frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi) V_d^\dagger(\pi)\right.$

$\left. = \frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi) V_d(\pi^{-1}) \right)$

$= \frac{1}{k!} \sum_{\pi \in S_k} \underbrace{sgn(\pi^{-1})}_{= sgn(\pi)} V_d(\pi)$

$= P^{(d,k)}_{asym}$.

NB5: $Im(P^{(d,k)}_{asym}) \subseteq Asym_k(\mathbb{C}^d)$

$\because$ $\forall \; |\psi\rangle \in (\mathbb{C}^d)^{\otimes k}$,

$P^{(d,k)}_{asym} |\psi\rangle \in ASym_k(\mathbb{C}^d)$

$\because$ $V_d(\pi) \; P^{(d,k)}_{asym} |\psi\rangle = sgn(\pi) \; P^{(d,k)}_{asym} |\psi\rangle$
$\forall \; \pi \in S_k$

(we used NB1, $V_d(\sigma) P_{asym} = sgn(\sigma) P_{asym}$)

NB6: $ASym_k(\mathbb{C}^d) \subseteq Im(P^{(d,k)}_{asym})$

$\because$ if $|\psi\rangle \in ASym_k(\mathbb{C}^d)$ then

$$P^{(d,k)}_{asym} |\psi\rangle = \frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi) V_d(\pi) |\psi\rangle$$

$$= \underbrace{\frac{1}{k!} \sum_{\pi \in S_k} sgn(\pi)^2}_{=1} |\psi\rangle$$

$$= |\psi\rangle.$$

$\square$

Proposition 20 (Dimension of the anti-symmetric subspace).

If $d \geq k$, then

$$tr(P^{(d,k)}_{asym}) = \dim(ASym_k(\mathbb{C}^d)) = \binom{d}{k}.$$

Else, $tr(P^{(d,k)}_{asym}) = 0$

Proof.

NB1: $ASym_k(\mathbb{C}^d) \overset{\text{Thm 19}}{=} Im(P^{(d,k)}_{asym})$

$$= span\{ P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle : \forall \; i_1 \dots i_k \in [d] \}$$

Goal: to count the # linearly independent vectors.

NB2: If $\exists$ two systems $l \neq m \in [k]$ s.t. $i_l = i_m$, then

$$P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle = 0.$$

$\Big(\because$ $P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle = P^{(d,k)}_{asym} V_d(\tau_{l,m}) |i_1\rangle \otimes \dots \otimes |i_k\rangle$

$\overset{(\text{Thm 19, NB2})}{=} \operatorname{sgn}(\tau_{l,m}) P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle$

$= - P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle \Big)$

$\therefore$ Thus all $i_1 \dots i_k$ must be distinct for $P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle \neq 0$.

NB3: If $d < k$, $\operatorname{tr}(P^{(d,k)}_{asym}) = 0$.

$\Big($ me: shouldn't $P^{(d,k)}_{sym} = 0$ $\because \forall |\psi\rangle$ $P^{(d,k)}_{sym} |\psi\rangle = 0$ when $d < k$ $\Big)$

case: $d \geq k$.

Suppose: $\forall$ $m \in [d]$

$\exists$ $|i_1\rangle \otimes \dots \otimes |i_k\rangle$ &

$|j_1\rangle \otimes \dots \otimes |j_k\rangle$ with $i_1, \dots i_k, j_1, \dots j_k \in [d]$

s.t. both sets $\{i_1, \dots i_k\}$ &

$\{j_1, \dots j_k\}$

contain $n_m \in \{0,1\}$ elements equal to m.

(i.e. whether or not $\exists$ l s.t. $i_l = j_l = m$.)

then: $\exists$ a permutation $V_d(\pi)$ s.t.

$$V_d(\pi) |i_1\rangle \otimes \dots \otimes |i_k\rangle = |j_1\rangle \otimes \dots |j_k\rangle$$

NB: $\because$ $P^{(d,k)}_{asym} V_d(\pi) = \operatorname{sgn}(\pi) P^{(d,k)}_{asym}$,

we have that

$$P^{(d,k)}_{asym} \underbrace{|i_1\rangle \otimes \dots \otimes |i_k\rangle} = \operatorname{sgn}(\pi) P^{(d,k)}_{asym} \underbrace{|j_1\rangle \otimes \dots \otimes |j_k\rangle}$$

$\Rightarrow$ $|i_1 \dots i_k\rangle$ & $|j_1 \dots j_k\rangle$ are linearly dependent.

Story: As before, we come up with a better labelling scheme, to label the distinct vectors.

Not^n: For $n_1 \dots n_d \in \{0,1\}$ with $n_1 + \dots + n_d = k$

we define $|n_1 \dots n_d\rangle := P^{(d,k)}_{asym} |i_1\rangle \otimes \dots \otimes |i_k\rangle$

where $i_1 \dots i_k$ is any (canonical) set s.t.

$\forall\ m \in [d]$,

$\exists\ n_m$ elements $j \in [k]$ s.t. $i_j = m$.

NB: It is easy to check that these vectors are orthogonal & thus independent.

NB2: The dimension is $\therefore$ given by the # of such vectors

= # of choosing an unordered subset of k elements from a set of d elements

$= \binom{d}{k}$.

$\square$

Story: We now look at the rel^n b/w the symmetric & anti-symmetric subspaces.

Proposition 21. It holds that $P^{(dk)}_{asym} + P^{dk}_{sym} = 0$.

In particular, $P^{(dk)}_{asym}$ & $P^{(dk)}_{sym}$ are orthogonal wrt Hilbert Schmidt norm.

Proof. We have

$$P^{(d,k)\dagger}_{asym} P^{(d,k)}_{sym} = \underset{\text{recall: self-adjoint}}{P^{(d,k)}_{asym}} P^{d,k}_{sym}$$

$$= \frac{1}{k!} \sum_{\pi \in S_k} \operatorname{sgn}(\pi) \underbrace{V_d(\pi) P^{(d,k)}_{sym}}_{\text{recall } P^{(d,k)}_{sym}}$$

$$= \underbrace{\left(\frac{1}{k!} \sum_{\pi \in S_k} \operatorname{sgn}(\pi) \right)}_{\text{by claim } 0} P^{(d,k)}_{sym}$$

proof of claim:
$$\frac{1}{k!} \sum_{\pi \in S_k} \operatorname{sgn}(\pi) = \frac{1}{k!} \sum_{\pi \in S_k} \operatorname{sgn}(\tau\pi)$$
$$= \operatorname{sgn}(\tau) \frac{1}{k!} \sum_{\pi \in S_k} \operatorname{sgn}(\pi)$$
$$= -\frac{1}{k!} \sum_{\pi \in S_k} \operatorname{sgn}(\pi)$$

□ □ where τ is any odd permutation

NB 1: For $k=2$ ($\&$ $d>1$),

$$\dim(\mathrm{Sym}_2(\mathbb{C}^d)) + \dim(\mathrm{ASym}_2(\mathbb{C}^d)) = \binom{d+1}{2} + \binom{d}{2}$$
$$= d^2$$
$$\Rightarrow \quad (\mathbb{C}^d)^{\otimes 2} = \mathrm{Sym}_2(\mathbb{C}^d) \oplus \mathrm{ASym}_2(\mathbb{C}^d)$$

NB 2: (i) since $P^{(d,2)}_{sym}$ & $P^{(d,2)}_{asym}$ are both linear combin^n of permutations,

they both commute with $U^{\otimes 2}$ $\forall\, U \in \mathbb{U}(d)$.

(ii) They are, thus, (a) elements of a basis for the $\mathrm{Comm}(\mathbb{U}(d), k=2)$ &

(b) orthogonal to each other.

(iii) The commutant can have dimension at most 2.

(recall: it is spanned by $\mathbb{1}$ & $\mathbb{F}$)

(iv) Thus, $P_{\mathrm{sym}}^{(d,k)}$ & $P_{\mathrm{asym}}^{(d,k)}$ form an orthonormal basis for the commutant.

(v) Since the moment operator is the orthogonal projector onto the commutant (Theorem 7), one can derive the formula for the second-order moment operator (already derived in Corollary 13), but this time using $P_{\mathrm{sym}}^{(d,k)}$ & $P_{\mathrm{asym}}^{(d,k)}$ as the basis.

$$\mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes 2}\, O\, U^{\dagger\otimes 2}\right] = \left\langle \frac{P_{\mathrm{sym}}^{(d,2)}}{\|P_{\mathrm{sym}}^{(d,2)}\|_2}, O\right\rangle_{HS} \frac{P_{\mathrm{sym}}^{(d,2)}}{\|P_{\mathrm{sym}}^{(d,2)}\|_2} +$$

(∵ orthonormal basis)

$$\left\langle \frac{P_{\mathrm{asym}}^{(d,2)}}{\|P_{\mathrm{asym}}^{(d,2)}\|_2}, O\right\rangle_{HS} \frac{P_{\mathrm{asym}}^{(d,2)}}{\|P_{\mathrm{asym}}^{(d,2)}\|_2}$$

(using $P_{\mathrm{sym}}^{\dagger} = P_{\mathrm{sym}}$ & $P_{\mathrm{sym}}^{2} = P_{\mathrm{sym}}$ & similarly for asym)

$$= \frac{\mathrm{tr}(P_{\mathrm{sym}}O)}{\mathrm{tr}(P_{\mathrm{sym}})} P_{\mathrm{sym}} + \frac{\mathrm{tr}(P_{\mathrm{asym}}O)}{\mathrm{tr}(P_{\mathrm{asym}})} P_{\mathrm{asym}}$$

using $P_{\mathrm{sym}}^{(d,2)} = \frac{1}{2}(\mathbb{1}+\mathbb{F})$ & $P_{\mathrm{asym}}^{(d,2)} = \frac{1}{2}(\mathbb{1}-\mathbb{F})$

$$= \frac{\mathrm{tr}(O) + \mathrm{tr}(\mathbb{F}O)}{d(d+1)}\left(\frac{\mathbb{1}+\mathbb{F}}{2}\right) + \frac{\mathrm{tr}(O) - \mathrm{tr}(\mathbb{F}O)}{d(d-1)}\left(\frac{\mathbb{1}-\mathbb{F}}{2}\right)$$

$$= \frac{\mathrm{tr}(O) - d^{-1}\,\mathrm{tr}(\mathbb{F}O)}{d^2-1}\mathbb{1} + \frac{\mathrm{tr}(O\mathbb{F}) - d^{-1}\mathrm{tr}(O)}{d^2-1}\mathbb{F}$$

Story: We finally show a theorem that states that
for all quantum states $|\phi\rangle$ in a
d-dimensional Hilbert space,
the moment operator of $|\phi\rangle\langle\phi|^{\otimes k}$ is
a uniform linear combination of permutations.
(which in turn is basically the projector on the
symmetric subspace $P^{(d,k)}_{Sym}$,
upto normalisation factors).

Theorem 22. Let $d, k \in \mathbb{N}$.
For all $|\phi\rangle \in \mathbb{C}^d$,
the moment operator is a uniform linear
combination of permutations, i.e.

$$\mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k}|\phi\rangle\langle\phi|U^{\otimes k\dagger}\right] = \frac{P^{(d,k)}_{Sym}}{\mathrm{tr}(P^{(d,k)}_{Sym})}$$

w/ $P^{(d,k)}_{Sym} = \frac{1}{k!}\sum_{\pi\in S_k} V_d(\pi)$ &

$$\mathrm{tr}(P^{(d,k)}_{Sym}) = \dim(\mathrm{Sym}_k(\mathbb{C}^d)) = \binom{k+d-1}{k}$$

again it looks it should be $\binom{k+d-1}{k-1}$

Proof. Recall: $\mathcal{M}^{(k)}_{\mu_H}(O) = \mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k} O U^{\otimes k\dagger}\right]$

$$= \sum_{\pi\in S_k} c_\pi(O)\, V_d(\pi)$$

Strategy: left multiply both sides by $V_d(\sigma^{-1})$ &
simplify.

NB1: $V_d(\sigma^{-1})\, \mathcal{M}^{(k)}_{\mu_H}\left((|\phi\rangle\langle\phi|)^{\otimes k}\right) = \mathcal{M}^{(k)}_{\mu_H}\left((|\phi\rangle\langle\phi|)^{\otimes k}\right)$

$\because$ (i) $V_d(\sigma^{-1})$ commutes w/ $U^{\otimes k}$ $\forall\, U$

(ii) $V_d(\sigma^{-1})\, |\phi\rangle^{\otimes k} = |\phi\rangle^{\otimes k}$.

NB2:
$$\sum_{\pi \in S_k} c_\pi\, V_d(\sigma^{-1})\, V_d(\pi)$$
$$= \sum_{\pi \in S_k} c_\pi\, V_d(\sigma^{-1}\pi) = \sum_{\pi \in S_k} c_{\sigma\pi}\, V_d(\pi)$$

NB3:
Combining [Recall], [NB1] & [NB2], we have

$$\mathcal{M}^{(k)}_{\mu_H}\left(|\phi\rangle\langle\phi|^{\otimes k}\right) = \sum_{\pi \in S_k} c_{\sigma\pi}\, V_d(\pi)$$

NB4 For $d > 1$,

[NB3] $\Rightarrow$ $c_\sigma = c_I$ $\quad\forall\, \sigma \in S_k$

(take σ to permute any two indices & take the difference; linear independence of $\{V_d(\pi)\}_\pi$ is not needed – just that they are distinct operators)

NB5 Thus, $\mathcal{M}^{(k)}_{\mu_H}\left(|\phi\rangle\langle\phi|^{\otimes k}\right) = c_I\left(\sum_{\pi \in S_k} V_d(\pi)\right)$

$$= c_I\, k!\, P^{(d,k)}_{Sym}.$$

The constants can be fixed by noting the tr of the RHS = 1

$\square$

Rough:

d fixed

$| \star | \star \star \star |$

fixed

$1 \ldots d$ labelled boxes

k stars

$$\binom{d+k-1}{k-1}$$

$$\binom{d+1}{2} + \binom{d}{2}$$

$$\frac{1}{2}\left[(d+1)\cdot(d) + d(d-1)\right]$$

$$\frac{1}{2}(d+1+d-1)\cdot d$$

$$d^2$$

$d+k-1$

$k-1$

$d+1 + d = 2d+1$