A

Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial

Anna
- Antonio Mele

§1 INTRODUCTION

Story: Haar measure formalises the fundamental concept of drawing unitary matrices uniformly at random.

: Applications include
- quantum tomography,
- computational advantage in random circuit sampling
- benchmarking quantum devices
- quantum foundations & communication
- quantum machine learning
- quantum many-body & high energy physics

Structure: §2. Overview of the notation & preliminary concepts

§3 Introduces the Haar measure w/ special focus on "moment operators" — useful quantities for evaluating Haar integrals.

§4 Symmetric & anti-symmetric spaces.

§ 5 vectorisation
§ 6 Tensor network based notation
] Tools for calculations

§ 7 unitary designs
§ 8 approximate unitary designs
§ 9 Applications.

Me: Here, I only plan to cover §2, 3 & 4.

§2 Notation & Preliminaries

Notation: $\mathcal{L}(\mathbb{C}^d)$ - linear operators acting on $\mathbb{C}^d$.
$\mathrm{Herm}(\mathbb{C}^d)$ - Hermitian
I - Identity operator
$\mathbb{I} := I \otimes I$ - Tensor product of two identity op.

$$\mathcal{U}(d) := \{ U \in \mathcal{L}(\mathbb{C}^d) : U^\dagger U = I \}.$$

$$[d] := \{1, \dots, d\}$$

Norms: Let $v \in \mathbb{C}^d$ be a vector &
$p \in [1, \infty]$.
p-norm of v: $\|v\|_p := \left(\sum_{i=1}^{d} |v_i|^p\right)^{1/p}$.

Schatten p-norm of $A \in \mathcal{L}(\mathbb{C}^d)$:

$$\|A\|_p := \mathrm{tr}\left(\left(\sqrt{A^\dagger A}\right)^p\right)^{1/p}$$

i.e. p-norm of singular values of A.

NB: Trace norm is $\|\cdot\|_1$, Hilbert Schmidt norm is $\|\cdot\|_2$.

Remark: the Hilbert-Schmidt norm is induced by the Hilbert Schmidt scalar product,

$$\langle A, B \rangle_{HS} := \mathrm{tr}(A^\dagger B) \quad \text{for} \quad A, B \in \mathcal{L}(\mathbb{C}^d).$$

NB: $\|\cdot\|_\infty$ the "infinite norm" is simply the largest singular value.

Remark: $\|\cdot\|_\infty$ can be seen as the limit of the Schatten p-norm as p approaches infinity.

Story: Here are some important facts about the Schatten p-norm that we will use.

claim 1: $\forall$ matrices A & $1 \leq p \leq q$,

it holds that

$$\|A\|_q \leq \|A\|_p$$

$$\|A\|_p \leq \mathrm{rank}(A)^{(p^{-1} - q^{-1})} \|A\|_q.$$

claim 2: $\forall$ unitaries U & V, $\forall$ the matrix A, it holds that

$$\|UAV\|_p = \|A\|_p.$$

claim 3: $\|A \otimes B\|_p = \|A\|_p \|B\|_p$ (tensor product property)

$\|AB\|_p \leq \|A\|_p \|B\|_p$ (submultiplicative property)

$\forall A, B \in \mathcal{L}(\mathbb{C}^d)$

Story: We now introduce some quantum notation.

Notation:
- $v \in \mathbb{C}^d$ is represented as $|v\rangle$ & its adjoint as $\langle v|$.
- $|\psi\rangle \in \mathbb{C}^d$ is a state if $\langle\psi|\psi\rangle = \||\psi\rangle\|_2 = 1$
- The canonical basis of $\mathbb{C}^d$ is denoted by $\{|i\rangle\}_{i=1}^d$.
- Maximally entangled (non-normalised) state is denoted as
$$|\Omega\rangle := \sum_{i=1}^d |i\rangle \otimes |i\rangle = \sum_{i=1}^d |ii\rangle.$$
- Set of quantum states
$$S(\mathbb{C}^d) := \{\rho \in \mathcal{L}(\mathbb{C}^d) : \rho \geq 0, \operatorname{tr}(\rho) = 1\}.$$
- A quantum channel $\Phi : \mathcal{L}(\mathbb{C}^d) \to \mathcal{L}(\mathbb{C}^d)$ is a linear map that is completely positive & trace preserving.
  i.e. $\forall$ positive operators $\sigma \in \mathcal{L}(\mathbb{C}^d \otimes \mathbb{C}^{d'})$
  $\forall\, d' \in \mathbb{N}$
  $(\Phi \otimes I)(\sigma)$ is also positive
  (maps $A \in \mathcal{L}(\mathbb{C}^{d'})$ to itself)

Claim: Every quantum channel Φ can be expressed in terms of d^2 Kraus operators,
i.e. $\exists\ \{K_i\}_{i=1}^{d^2}$ operators
s.t. $$\Phi(\cdot) = \sum_{i=1}^{d^2} K_i (\cdot) K_i^\dagger$$
where $\sum_{i=1}^{d^2} K_i^\dagger K = \mathbb{1}$ (to ensure trace is preserved)

§3 Haar Measure & the Moment operator

Def^n 1 (Haar Measure).

The Haar measure on the unitary group $\mathbb{U}(d)$ is the unique probability measure μ_H that is both left & right invariant over the group $\mathbb{U}(d)$,

i.e. $\forall$ integrable functions f & $\forall\ V \in \mathbb{U}(d)$, it holds that

$$\int_{\mathbb{U}(d)} f(U)\, d\mu_H(U) = \int_{\mathbb{U}(d)} f(UV)\, d\mu_H(U)$$

$$= \int_{\mathbb{U}(d)} f(VU)\, d\mu_H(U). \qquad (1)$$

Imp. claim: For compact groups (such as the unitary group), there exists a unique prob. measure that is both left & right invariant under group multiplication.

NB: Since the Haar measure is a prob. measure, it satisfies

(a). $\int_S 1\, d\mu_H(U) \geq 0$ $\forall$ sets $S \subseteq \mathbb{U}(d)$ &

(b). $\int_{\mathbb{U}(d)} 1\, d\mu_H(U) = 1.$

Notation: This is why we use $\mathbb{E}_{U \sim \mu_H}[f(U)] = \int_{\mathbb{U}(d)} f(U)\, d\mu_H(U)$ (as in, "it's a measure") (2)

Remark: When $f(U)$ is a matrix valued fn,
the expected value is understood to be
the expected value of each of its entries.

Story: We can prove that unbalanced products of matrices vanishes,
i.e. the following holds.

Proposition 2. Let $k_1, k_2 \in \mathbb{N}$.
If $k_1 \neq k_2$ then it holds that

$$\mathop{\mathbb{E}}_{U \sim \mu_H} \left[U^{\otimes k_1} \otimes U^{* \otimes k_2} \right] = 0 .$$

Proof. Replace U with $U e^{i \frac{\pi}{k_1 - k_2}}$

NB: This doesn't change the value of the integral
by right multiplication invariance of the
Haar measure, i.e.

$$\mathop{\mathbb{E}}_{U \sim \mu_H} \left[U^{\otimes k_1} \otimes U^{* \otimes k_2} \right] = - \mathop{\mathbb{E}}_{U \sim \mu_H} \left[U^{\otimes k_1} \otimes U^{* \otimes k_2} \right] \quad (3)$$

□

Story: The next proposition helps in subsequent calculations.
It shows that in Haar integrals,
we are free to replace U with $U^\dagger$

Proposition 3. For all integrable functions f defined on $U(d)$,
it holds that $\mathop{\mathbb{E}}_{U \sim \mu_H} \left[f(U^\dagger) \right] = \mathop{\mathbb{E}}_{U \sim \mu_H} \left[f(U) \right]$. (4)

[Proof. Let: μ_+ be the prob. measure, defined as follows:

$$\int_{U(d)} f(U)\, d\mu_+(U) := \int_{U(d)} f(U^+)\, d\mu(U).$$

Strategy: We show that μ_+ is right & left invariant.

Since the Haar measure is the unique measure
that satisfies this property,
we can then conclude μ_+ is the same as μ.

Let: V be a fixed unitary.

NB: $\int_{U(d)} f(UV)\, d\mu_+(U) = \int_{U(d)} f(U^+V)\, d\mu_H(U)$ (by def^n)

$$= \int_{U(d)} f(U^+V^+V)\, d\mu_H(U) \quad \begin{matrix}(\text{right inv of } d\mu_H) \\ U \to VU \\ \text{so} \\ U^+ \to U^+V^+\end{matrix}$$

$$= \int_{U(d)} f(U^+)\, d\mu_H(U)$$

$$= \int_{U(d)} f(U)\, d\mu_+(U) \quad (\text{by def}^n)$$

□

Story: A quantity that plays a crucial role in our analysis,
is the k-th moment operator,
(where k is a natural number).

Def^n 4 (k^{th} Moment operator).

Fix a probability measure μ_H.

The k-th moment operator,

$$\mathcal{M}^{(k)}_{\mu_H} : \mathcal{L}((\mathbb{C}^d)^{\otimes k}) \to \mathcal{L}((\mathbb{C}^d)^{\otimes k})$$

is defined as

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

$\forall$ operators $O \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$.

Story: • By characterising the moment operator & computing its matrix elements, one can explicitly evaluate integrals over the Haar measure.

• To see this, consider the e.g. where

$$O := |i_1 \dots i_k\rangle\langle j_1 \dots j_k|$$

where $i_1 \dots i_k \in [d]$ & also $j_1 \dots j_k \in [d]$

Then, we have

$$\langle l_1 \dots l_k | \mathop{\mathbb{E}}_{U \sim \mu_H} \left[U^{\otimes k} \, O \, U^{\dagger \otimes k} \right] | m_1 \dots m_k \rangle$$

$$= \mathop{\mathbb{E}}_{U \sim \mu_H} \left[U_{l_1 i_1} \dots U_{l_k i_k} \, U^*_{m_1 j_1} \dots U^*_{m_k j_k} \right] \quad [a]$$

where $l_1 \dots l_k \in [d]$ & also $m_1 \dots m_k \in [d]$.

• To characterise the moment operator,
we need to define the
k-th order commutant of a set of matrices S.

Def^n 5 (Commutant).
Given $S \subseteq \mathcal{L}(\mathbb{C}^d)$,
define its k^{th} order commutant as

$$\mathrm{Comm}(S,k) := \{ A \in \mathcal{L}((\mathbb{C}^d)^{\otimes k}) : [A, B^{\otimes k}] = 0 \ \forall B \in S \}$$

NB: The commutant is a vector space.
$\hookrightarrow \mathrm{Comm}(S,k)$ ✓

Story: Now, we see that
the moment operator is
an orthogonal projector onto
the commutant of the unitary group,
(i.e. $\mathrm{Comm}(U(d),k)$)
w.r.t. the Hilbert-Schmidt innerproduct.
• To this end, we first prove the following lemma.

Lemma 6 (Properties of the moment operator).
The moment operator $\mathcal{M}^{(k)}_{\mu_H}(\cdot) := \mathop{\mathbb{E}}_{U\sim\mu_H}[U^{\otimes k}(\cdot)U^{\dagger\otimes k}]$
has the following properties:

1. $\mathcal{M}$ is linear, trace-preserving, and self-adjoint wrt the Hilbert-Schmidt inner product.

2. For all $A \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$,

$$\mathcal{M}^{(k)}_{HH}(A) \in \mathrm{Comm}(U(d), k)$$

3. If $A \in \mathrm{Comm}(U(d), k)$, then

$$\mathcal{M}^{(k)}_{HH}(A) = A$$

Proof.

1. Linearity & trace preservation, follow from the definition of $\mathcal{M}^{(k)}_{HH}(\cdot)$ (see page 9)

To show that the moment operator is self-adjoint, we need to prove that (we use $\mathcal{M}_k(\cdot)$ to be brief.)

$$\langle \mathcal{M}_k(A), B\rangle_{HS} = \langle A, \mathcal{M}_k(B)\rangle_{HS} \quad \forall\, A, B \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$$

To this end, we have

$$\mathrm{tr}(\mathcal{M}_k^\dagger(A)\, B) = \mathop{\mathbb{E}}_U \mathrm{tr}(U^{\otimes k} A^\dagger U^{\dagger\otimes k} B)$$

$$= \mathrm{tr}\left(A^\dagger \mathop{\mathbb{E}}_U (U^{\dagger\otimes k} B U^{\otimes k})\right)$$

$$= \mathrm{tr}(A^\dagger \mathcal{M}_k(B)) \quad \text{(using Prop 3)}$$

2. $\mathcal{M}_k(A) \in \mathrm{Comm}(U(d), k)$

$\Leftrightarrow V^{\otimes k} \mathcal{M}_k(A) V^{\dagger\otimes k} = \mathcal{M}_k(A) \quad \forall\ V \in U(d)$

$\Leftrightarrow V^{\otimes k} \mathcal{M}_k(A) = \mathcal{M}_k(A) V^{\otimes k} \quad \forall\ V \in U(d)$

NB: $V^{\otimes k}\, \mathcal{M}_k(A) = \mathop{\mathbb{E}}_U V^{\otimes k} U^{\otimes k} A\, U^{\dagger \otimes k}$

$= \mathop{\mathbb{E}}_U V^{\otimes k} V^{\dagger \otimes k} U^{\otimes k} A\, U^{\dagger \otimes k} V^{\otimes k}$

(using left invariance of the Haar measure $\mathop{\mathbb{E}}_U f(U) = \mathop{\mathbb{E}}_U f(V^\dagger U)$) $= \mathop{\mathbb{E}}_U U^{\otimes k} A\, U^{\dagger \otimes k} V^{\otimes k}$

$= \mathcal{M}_k(A)\, V^{\otimes k}$.

3. If $A \in \mathrm{Comm}(U(d), k)$ then

$$\mathcal{M}_k(A) = A$$

This is because $\forall U$, $U^{\otimes} A U^{\dagger \otimes k} = A$, $\because [A, U^{\otimes}] = 0$, $A \in \mathrm{Comm}(U(d), k)$

$$\Rightarrow \mathop{\mathbb{E}}_U U^{\otimes} A\, U^{\dagger \otimes k} = A$$

$$\| \quad \mathcal{M}_k(A)$$

□

Thm 7 (Projector onto the commutant)

The moment operator $\mathcal{M}^{(k)}_{\mu_H}(\cdot) \overset{\text{recall}}{=} \mathop{\mathbb{E}}_{U \sim \mu_H} [U^{\otimes k} (\cdot)\, U^{\dagger \otimes k}]$

is the orthogonal projector onto the commutant

$$\mathrm{Comm}(U(d), k) = \mathrm{Comm}$$

wrt the Hilbert-Schmidt inner product

In particular, let • $P_1 \ldots P_{\dim(\mathrm{Comm})}$ be an orthonormal basis of Comm &

• $O \in \mathcal{I}((\mathbb{C}^d)^{\otimes k})$.

Then, it holds that

$$\mathcal{M}^{(k)}_{HH}(O) = \sum_{i=1}^{\dim(\mathrm{Comm})} \langle P_i, O\rangle_{HS} P_i .$$

Proof.

Extend the orthonormal basis of the commutant to be that of $\mathcal{L}((\mathbb{C}^d)^{\otimes k}) =: V$, as follows:

$$P_1, \quad P_{\dim(\mathrm{Comm})}, P_{\dim(\mathrm{Comm})+1}, \cdots P_{\dim(V)}$$

Now, $\mathcal{M}_k(O) = \sum_{i=1}^{\dim(V)} \langle P_i, \mathcal{M}_k(O)\rangle_{HS} P_i$

$$= \sum_{i=1}^{\dim(\mathrm{Comm})} \langle P_i, \mathcal{M}_k(O)\rangle_{HS} P_i +$$

$$\underbrace{\sum_{i=\dim(\mathrm{Comm})+1}^{\dim V} \langle P_i, \mathcal{M}_k(O)\rangle_{HS} P_i}_{=0 \;\because\; \mathcal{M}_k(O) \in \mathrm{Comm} \text{ (Lemma 6.2).}}$$

$$= \sum_{i=1}^{\dim(\mathrm{Comm})} \langle \mathcal{M}_k(P_i), O\rangle_{HS} P_i \quad \because \mathcal{M}_k(\cdot) \text{ is self-adjoint}$$

$$= \sum_{i=1}^{\dim(\mathrm{Comm})} \langle P_i, O\rangle_{HS} P_i \quad \because P_i \in \mathrm{Comm}\ \forall i \in \{1, \dim(\mathrm{Comm})\} \ \&\ \mathcal{M}_k(A) = A \ \forall A \in \mathrm{Comm}$$

□

Story. We just saw how the moment operator is intimately related to the k-order commutant of the unitary group (i.e. operators that commute w/ $U^{\otimes k}$).

- A set of operators that certainly commutes with $U^{\otimes k}$ is the permutation among the tensor products.

• We now define permutation operators.

Defⁿ 8 (Permutation operators). Given $\pi \in S_k$, an element of the symmetric group S_k, we define the permutation matrix $V_d(\pi)$ as follows:

$$V_d(\pi)\, |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle = |\psi_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes |\psi_{\pi^{-1}(k)}\rangle$$

$\forall \quad |\psi_1\rangle \ldots |\psi_k\rangle \in \mathbb{C}^d$.

NB: $V_d(\sigma)\, V_d(\pi) = V_d(\sigma\pi)$

$V_d(\pi^{-1}) = V_d^\dagger(\pi)$

$$V_d(\pi) = \sum_{i_1 \ldots i_k \in [d]^k} |i_{\pi^{-1}(1)} \cdots i_{\pi^{-1}(k)}\rangle\langle i_1 \ldots i_k|.$$

$$V_d(\pi)\,(A_1 \otimes \cdots \otimes A_k)\, V_d^\dagger(\pi) = A_{\pi^{-1}(1)} \otimes \cdots \otimes A_{\pi^{-1}(k)}.$$

$\forall\ A_1, \ldots, A_k \in \mathcal{L}(\mathbb{C}^d)$

Story: Surprisingly, it turns out that permutation operators characterize all possible matrices in the commutant — this is the Schur-Weyl duality.

Theorem 9 (Schur-Weyl duality). The k-th order commutant of the unitary group is the span of permutation operators associated with S_k:

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

Story: We omit the general proof
but do prove the $k=1$ & $k=2$ case later.

: One side of the proof is easy to see though,
i.e. $\text{span}\{V_d(\pi) : \pi \in S_k\} \subseteq \text{Comm}(U(d), k)$.

NB: It suffices to show that $[V_d(\pi), U^{\otimes k}] = 0$.

To this end, observe that

$$V_d(\pi)\left(U^{\otimes k} |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle\right) = V_d(\pi)\left(U|\psi_1\rangle \otimes \cdots \otimes U|\psi_k\rangle\right)$$

$$= U|\psi_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes U|\psi_{\pi^{-1}(k)}\rangle$$

$$= U^{\otimes k} V_d(\pi)\left(|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle\right)$$

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

NB2: Even though Permutation Matrices form a basis for the
k-th order commutant of the unitary group,
they are not orthonormal wrt. the Hilbert-Schmidt
inner product.

Story: One cannot, therefore, apply Theorem 7 directly.
Nonetheless, there is an alternate approach that
allows one to evaluate the moment operators &
thus integrals over the Haar Measure.

Theorem 10 (computing moments).

Let $O \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$.

The moment operator can then be expressed as a linear combination of permutation operators:

$$M_{\mu_n}^{(k)}(O) \overset{\text{recall}}{=} \mathop{\mathbb{E}}_{U \sim \mu_n} \left[U^{\otimes k} O U^{\dagger \otimes k} \right] = \sum_{\pi \in S_k} c_\pi(O) \, V_d(\pi) \tag{30}$$

where the coefficients $c_\pi(O)$ can be computed by solving the following linear system of $k!$ equations:

$$\mathrm{tr}\left(V_d^\dagger(\sigma) O \right) = \sum_{\pi \in S_k} c_\pi(O) \, \mathrm{tr}\left(V_d^\dagger(\sigma) V_d(\pi) \right) \tag{31}$$

$$\forall \ \sigma \in S_k .$$

The system always has at least one solution.

Proof. Eq (30) follows from • Lemma 6.2 (which says $M_k(O) \in \mathrm{comm}(U^{\otimes}(d), k)$)

&

• Schur-Weyl duality (Theorem 9 which says permutations span $\mathrm{comm}(U^{\otimes}(d), k)$)

To get Eq (31), proceed as follows:

$$\mathop{\mathbb{E}}_{U} V_d^\dagger(\sigma) U^{\otimes k} O U^{\dagger \otimes k} = \sum_{\pi} c_\pi(O) \, V_d^\dagger(\sigma) V_d(\pi)$$

(left multiply (30) w $V_d^\dagger$)

$$\mathop{\mathbb{E}}_{U} U^{\otimes k} V_d^\dagger(\sigma) O U^{\dagger \otimes k}$$

(i.e. permutations commute with $U^{\otimes k}$)

$$\Rightarrow \quad \mathrm{tr}\left(V_d^\dagger(\sigma) O \right) = \sum_{\pi} c_\pi(O) \, \mathrm{tr}\left(V_d^\dagger(\sigma) V_d(\pi) \right).$$

Finally, a solution to the linear system exists $\therefore M_k(O) \in \text{span}\{V_d(\pi) : \pi \in S_k\}$

□

Story: (i) The previous theorem can be used to explicitly evaluate the coefficients

$c_\pi(O)$ (in the permutation basis expansion of a moment op O)

as $$c_\pi(O) = \sum_{\sigma \in S_k} (G^\dagger)_{\pi,\sigma} \, \text{tr}(V_\sigma^\dagger O)$$

(permutation matrix)

where $G_{\pi,\sigma} := \text{tr}(V_\sigma^\dagger(\pi) V_d(\sigma))$ &
$= \text{tr}(V_d(\pi^{-1}\sigma))$

$G^\dagger$ is its pseudo-inverse.

(ii) $(G^\dagger)_{\pi,\sigma} =: Wg(\pi^{-1}\sigma, d)$ is written in terms of "Weingarten coefficients" which in turn can be written in terms of "characters of the symmetric gp".

Details beyond this are outside the scope of this tutorial

(iii) The gram matrix G, does have a simple expression in terms of the cyclic structure of the permutations, given by

$$G_{\pi,\sigma} = \text{tr}(V_d(\pi^{-1}\sigma)) = d^{\#\text{cycles}(\pi^{-1}\sigma)}$$

$\because$ NB: $\text{tr}(V_d(\pi)) = \sum_{i_1,\dots,i_k \in [d]} \langle i_1 | i_{\pi^{-1}(1)} \rangle \dots \langle i_k | i_{\pi^{-1}(k)} \rangle$

&

NB2: The sum has $d^{\#\text{cycles}(\pi)}$ non-vanishing terms & they are all equal to 1.

(look at the rough page & work out a few examples to convince yourself).

Prop. 11. For $\pi \in S_k$, the permutation matrices $V_d(\pi)$ are linearly independent if $k \leq d$ but linearly dependent if $k > d$.

Proof.

Case. $k \leq d$.

Suppose: The permutations $\{V_d(\pi)\}_\pi$ are indeed linearly dependent,

i.e. $\exists\ \alpha_\pi \in \mathbb{C},\ \forall\ \pi \in S_k$ s.t

$$\sum_{\pi \in S_k} \alpha_\pi V_d(\pi) = 0.$$

choose: k distinct elements $i_1, \dots, i_k \in [d]$ (which we can because $k \leq d$)

NB: $$\sum_{\pi \in S_k} \alpha_\pi V_d(\pi) |i_1 \dots i_k\rangle = \sum_{\pi \in S_k} \alpha_\pi |i_{\pi^{-1}(1)} \dots i_{\pi^{-1}(k)}\rangle$$

NB2: Left multiply this ↗ w/ $\langle i_{\sigma^{-1}(1)} \dots i_{\sigma^{-1}(k)}|$

$\alpha_\sigma = 0$

(∵ $\langle i_{\sigma^{-1}(1)} \dots i_{\sigma^{-1}(k)} | i_{\pi^{-1}(1)} \dots i_{\pi^{-1}(k)}\rangle = 0$ if $\sigma \neq \pi$ & $= 1$ if $\sigma = \pi$)

NB3: This holds for all σ, i.e. $\alpha_\sigma = 0\ \forall\ \sigma$.

conclusion: $V_d(\pi)$ are linearly independent if $k \leq d$.

Case: $k > d$.

Consider: $A = \sum_{\pi \in S_k} \operatorname{sgn}(\pi)\, V_d(\pi)$

Strategy: We show this linear combination is the zero operator – explicitly showing coefficients $\alpha_\pi := \operatorname{sgn}(\pi)$ yield a linear dependence among $\{V_d(\pi)\}_\pi$.

Consider: The action of A on any product basis state $|i_1\rangle \otimes \cdots \otimes |i_k\rangle$.

NB: $\exists\ l \neq m \in [k]$ s.t. $i_l = i_m$

i.e. there are two "systems" with the same "i".

(∵ $k > d$, they must repeat)

Strategy: We use anti-symmetrisation, to prove $A = 0$.

NB: ($\tau_{l,m}$ swaps systems $l \& m$)

$$\begin{aligned} A|i_1 \cdots i_k\rangle &= A\, V_d(\tau_{l,m})\, |i_1 \cdots i_k\rangle \\ &= \sum_{\pi \in S_k} \operatorname{sgn}(\pi)\, V_d(\pi)\, V_d(\tau_{l,m})\, |i_1 \cdots i_k\rangle \\ &= \sum_{\pi \in S_k} \operatorname{sgn}(\pi)\, V_d(\pi \tau_{l,m}) |i_1 \cdots i_k\rangle \\ &= \sum_{\pi \in S_k} \operatorname{sgn}(\pi \tau_{l,m}^{-1}) V_d(\pi)\, |i_1 \cdots i_k\rangle \\ &= \operatorname{sgn}(\tau_{l,m}^{-1}) \sum_{\pi} \operatorname{sgn}(\pi) V_d(\pi) |i_1 \cdots i_k\rangle \\ &= -A\, |i_1 \cdots i_k\rangle \end{aligned}$$

i.e. $A|i_1 \cdots i_k\rangle = 0$

Conclusion: since $|i_1 \dots i_k\rangle$ was arbitrary, $A = 0$.

: $\{V_d(\pi)\}$ are linearly dependent when $k > \pi$.

□

Story: Still be useful to define the identity & swap (or "flip") operators for two-subsystem systems, (i.e. corresponding to S_2).

Defⁿ 12 (Identity & Flip operators).

The identity operator $\mathbb{I}$ is defined as

$$\mathbb{I}(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\phi\rangle \quad \forall\ |\psi\rangle, |\phi\rangle \in \mathbb{C}^d.$$

The flip operator $\mathbb{F}$ is defined as

$$\mathbb{F}(|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle \quad \forall\ |\psi\rangle, |\phi\rangle \in \mathbb{C}^d.$$

NB: In the computational basis, one can equivalently write

$$\mathbb{I} = \sum_{i,j=1}^{d} |ij\rangle\langle ij| \quad , \quad \mathbb{F} = \sum_{i,j=1}^{d} |ij\rangle\langle ji|$$

NB2: "Swap trick". $\mathrm{tr}((A \otimes B)\mathbb{F}) = \mathrm{tr}(AB)$

Hint: $\langle ij| A \otimes B |ji\rangle = \langle i|A|j\rangle \langle j|B|i\rangle$

Story: • Turns out to be very helpful & is used extensively later.

• We now look at a corollary of Theorem 10 which turns out to be useful later.

Corollary 13 (First & second moment), assumes $d > 1$ (for an n-qubit system, $d = 2^n > 1$).

(i) Given $O \in \mathcal{L}(\mathbb{C}^d)$, it holds that

$$\mathop{\mathbb{E}}_{U \sim \mu_H} [U O U^\dagger] = \frac{\mathrm{tr}(O)}{d} \cdot \mathbb{I}$$

(ii) Given $O \in \mathcal{L}((\mathbb{C}^d)^{\otimes 2})$, it holds that

$$\mathop{\mathbb{E}}_{U \sim \mu_H} [U^{\otimes 2} O U^{\dagger \otimes 2}] = c_{\mathbb{I},O}\, \mathbb{I} + c_{F,O}\, F$$

where

$$c_{\mathbb{I},O} = \frac{\mathrm{tr}(O) - d^{-1}\mathrm{tr}(FO)}{d^2 - 1} \quad \&$$

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

[Proof.

(i) Recall: Thm 10 says $\mathop{\mathbb{E}}_{U \sim \mu_H} [U O U^\dagger] \in \mathrm{span}\{\text{permutation operators on } S_1\}$

NB S_1 has only the identity operation

Thus: $\mathop{\mathbb{E}}_{U \sim \mu_H} [U O U^\dagger] = c_I \cdot \mathbb{I}$

& by taking the trace, we have that $\mathrm{tr}(O) = c_I \cdot d$

i.e. $c_I = \frac{\mathrm{tr}(O)}{d}$

(ii) Story: Proceeding similarly,

NB: S_2 has only $\mathbb{I}$ & F as the corresponding permutations.

$$\therefore \mathop{\mathbb{E}}_{U \sim \mu_H} [U^{\otimes 2} O U^{\dagger \otimes 2}] = c_{\mathbb{I},O}\, \mathbb{I} + c_{F,O}\, F$$

$\in \mathbb{C}$

strategy: To find these coefficients, we can

(i) tr both sides

(ii) multiply w/ F & tr both sides.

NB: Proceeding as described, one gets

$$\mathrm{tr}(O) = C_{\mathbb{I},0}\, d^2 + C_{F,0}\, d \qquad \text{(recall: } \mathrm{tr}(A\otimes B\, F) = \mathrm{tr}(AB)\text{)}$$

$$\mathrm{tr}(FO) = C_{\mathbb{I},0}\, d + C_{F,0}\, d^2$$

∴ this can be solved to obtain

$$C_{\mathbb{I},0} = \frac{\mathrm{tr}(O) - d^{-1}\mathrm{tr}(OF)}{d^2-1} \quad \&$$

$$C_{F,0} = \frac{\mathrm{tr}(FO) - d^{-1}\mathrm{tr}(O)}{d^2-1}$$

(me: I didn't check this myself)

□

Rough

$$\mathrm{tr}\left(V_d(\pi)\right) = \sum_{i_1, \ldots, i_k \in [d]} \langle i_1 | i_{\pi^{-1}(1)} \rangle \cdots \langle i_k | i_{\pi^{-1}(k)} \rangle$$

$\mathbb{I}$ $\quad$ d $\quad$ sys 1 $\quad$ $\langle 0|0\rangle \langle 0|0\rangle$

d $\quad$ sys 2 $\quad$ $\langle 0|0\rangle \langle 1|1\rangle$

d $\quad$ sys 3 $\quad$ $\langle 1|1\rangle$

d^3

d $\quad$ sys 1 $\quad$ $\langle 0|0\rangle \langle 0|0\rangle$

sys 2 $\quad$ $\langle 0|1\rangle \langle 1|0\rangle$

d $\quad$ $\langle 1|1\rangle$

when $i_1 \ldots i_k$ distinct, contribution if $\pi = \mathbb{I}$, 0 else.

$i_1 = i_2 \neq i_3 \neq i_4 \ldots \neq i_k$, Then

when (a) $\mathbb{I}$ rest &

cycle along 1 & 2 — 1

(b) $\mathbb{I}$ anywhere.

. . . . .