

Randomness in Quantum Information and Many-Body Physics

Xhek Turkeshi^{*} and Markus Heinrich[†]

Institute for Theoretical Physics, University of Cologne, ZùlpicherstraÙe 77a, 50937 Kùln,
Germany

^{*} xturkesh@uni-koeln.de , [†] markus.heinrich@uni-koeln.de

Abstract

These lecture notes develop a self-contained route from Haar-random unitaries to quantitative diagnostics of randomness in quantum many-body systems. The first part introduces permutation representations, graphical replica calculus, Weingarten integration, and unitary designs. The second turns these tools into classical-shadow estimators and moment-operator bounds for local random circuits. The final part studies anticoncentration, random matrix-product states, magic, entanglement growth, and out-of-time-ordered correlators. The presentation targets Master's students with introductory quantum mechanics and linear analysis as prerequisites; intermediate algebra, regimes of validity, graphical derivations, and graded exercises are included throughout.

Revision convention. Text, formulas, headings, and exercises added or substantially rewritten in this edition are printed in red. Unchanged material from the working manuscript remains black.

Contents

1	About this course	3
1.1	How to use these notes	3
1.2	Global notation	3
2	Quantum Randomness I	4
2.1	What is a Haar measure?	4
2.2	Permutations and their combinatorics	7
2.2.1	Permutations and Cycles	7
2.2.2	The Action of Permutations on Quantum States	13
2.3	Weingarten calculus	17
2.4	Approximating the Haar measure: Unitary designs	20
2.5	The Clifford group	22
2.6	Exercises	24
2.7	Supplementary exercises: permutations and replica calculus	24
2.8	Further reading	26
2.9	Cumulative exercises: Quantum Randomness I	26
3	Measuring Properties using Classical Shadows	28
3.1	Reconstructing quantum states from measurements	28
3.2	Shadow estimation with randomized measurements	30
3.2.1	Clifford measurements	32
3.2.2	Pauli measurements	37
3.2.3	Beyond linear observables: estimating purity	38

2.2.2 The Action of Permutations on Quantum States

Throughout this course, we work with a d -dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$, with orthonormal basis $\{|x\rangle\}_{x=0}^{d-1}$. Its k -fold tensor power $\mathcal{H}^{\otimes k}$ is called the *replica space*. A permutation $\sigma \in S_k$ acts by moving the content of slot j to slot $\sigma(j)$:

$$R_\sigma |x_1, \dots, x_k\rangle = |x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(k)}\rangle. \quad (53)$$

The inverse is essential. For example, if $\sigma = (1\ 4\ 3)(2)$, then $1 \mapsto 4$, $4 \mapsto 3$, and $3 \mapsto 1$; therefore

$$R_\sigma |x_1, x_2, x_3, x_4\rangle = |x_3, x_2, x_4, x_1\rangle. \quad (54)$$

With the usual convention $(\sigma\pi)(j) = \sigma(\pi(j))$, Eq. (53) defines a unitary representation:

$$R_{\sigma\pi} = R_\sigma R_\pi, \quad R_i = \mathbb{1}, \quad R_{\sigma^{-1}} = R_\sigma^{-1} = R_\sigma^\dagger. \quad (55)$$

Indeed,

$$R_\sigma R_\pi |x_1, \dots, x_k\rangle = |x_{\pi^{-1}(\sigma^{-1}(1))}, \dots, x_{\pi^{-1}(\sigma^{-1}(k))}\rangle \quad (56)$$

$$= |x_{(\sigma\pi)^{-1}(1)}, \dots, x_{(\sigma\pi)^{-1}(k)}\rangle = R_{\sigma\pi} |x_1, \dots, x_k\rangle. \quad (57)$$

This calculation also fixes the convention used in every later replica formula.

We leave the verification of the other axioms – such as unitarity and inverse consistency – as an exercise.

Exercise 2.5. Verify that R defines a unitary representation of the symmetric group S_k , i.e., check Eq. (55).

Exercise 2.6. Show that permutations act on tensor products of operators as follows:

$$R_\sigma (A_1 \otimes A_2 \otimes \dots \otimes A_k) R_\sigma^\dagger = A_{\sigma^{-1}(1)} \otimes A_{\sigma^{-1}(2)} \otimes \dots \otimes A_{\sigma^{-1}(k)}. \quad (58)$$

Hint: Apply both sides to a product basis state.

Composite Systems In practice, we often work with *multi-qudit systems* described by a Hilbert space of the form $\mathcal{H} = (\mathbb{C}^q)^{\otimes n}$, corresponding to n qudits of local dimension q . In this setting, the k -fold copy of the system is given by the tensor product

$$((\mathbb{C}^q)^{\otimes n})^{\otimes k}, \quad (59)$$

which can be naturally visualized as a $k \times n$ grid of qudits (see Fig. 1). Each row represents one replica of the full system, and each column represents the k copies of a single local qudit.

Quantum operations such as global unitaries typically act *row-wise*, that is, identically and independently on each copy. Such operations are of the form

$$U^{\otimes k}, \quad \text{where } U \in U((\mathbb{C}^q)^{\otimes n}), \quad (60)$$

meaning that the unitary acts in parallel across the k rows.

In contrast, permutations act by permuting the *rows*, i.e., the k copies of each local qudit. This operation is performed *column-wise*, and can be implemented by applying the same permutation operator to each column in parallel. This leads to a convenient factorized structure: if we reinterpret the total space via the isomorphism

$$((\mathbb{C}^q)^{\otimes n})^{\otimes k} \simeq ((\mathbb{C}^q)^{\otimes k})^{\otimes n}, \quad (61)$$

then the permutation operator R_π acting on the full system decomposes as

$$R_\pi = r_\pi^{\otimes n}, \quad (62)$$

Here r_π permutes the k replicas of one local qudit: it acts on $(\mathbb{C}^q)^{\otimes k}$, a space of dimension q^k (not dimension k). This “horizontal” factorization is exactly what is depicted in Fig. 1 and will be essential in constructing efficient representations of randomized operations throughout the course.

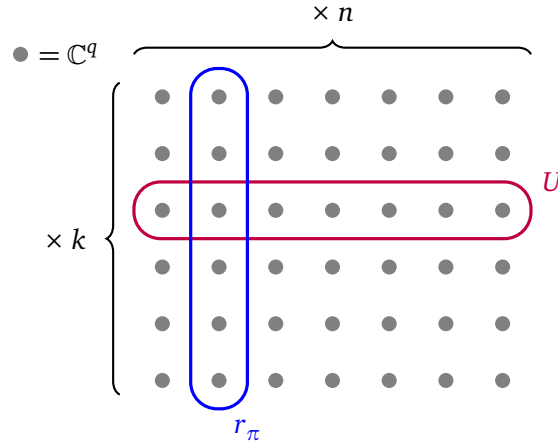


Figure 1: The Hilbert space $((\mathbb{C}^q)^{\otimes n})^{\otimes k}$ depicted as a $k \times n$ grid where every point corresponds to a copy of $\mathbb{C}^q$. Unitaries $U \in \text{U}(q^n)$ act row-wise on the grid, while permutations $\pi \in S_k$ act column-wise.

Traces Traces will play a fundamental role for explicit computations. Here, we derive a formula for the trace of permutation operators and for the trace of a product operator multiplied with a permutation. Let us first consider the cyclic permutation $\gamma = (k, k-1, \dots, 1)$. Then, we compute

$$\begin{aligned} \text{tr}(R_\gamma) &= \sum_{x_1, \dots, x_k=0}^{d-1} \langle x_1, \dots, x_k | R_\gamma | x_1, \dots, x_k \rangle \\ &= \sum_{x_1, \dots, x_k} \langle x_1, \dots, x_k | x_2, \dots, x_k, x_1 \rangle = \sum_{x_1, \dots, x_k} \delta_{x_1, x_2} \delta_{x_2, x_3} \dots \delta_{x_{k-1}, x_k} \delta_{x_k, x_1} = d. \end{aligned} \quad (63)$$

Next, consider an arbitrary permutation σ . Then, we can find a permutation π such that $\pi\sigma\pi^{-1} = (1, \dots, b_1)(b_1+1, b_1+2, \dots, b_2) \dots (b_{r-1}+1, b_{r-1}+2, \dots, b_r)$ where $r = \#\sigma$ is the number of cycles in σ (recall that the cycle structures of σ and $\pi\sigma\pi^{-1}$ have to necessarily match, cf. Ex. 2.3). But $R_{\pi\sigma\pi^{-1}}$ is simply a tensor product of cyclic permutations on $\mathcal{H}^{\otimes b_1}, \dots, \mathcal{H}^{\otimes(b_2-b_1)}, \dots, \mathcal{H}^{\otimes(b_r-b_{r-1})}$ and thus

$$\text{tr}(R_\sigma) = \text{tr}(R_{\pi\sigma\pi^{-1}}) = \prod_{i=1}^r d = d^r = d^{\#\sigma}. \quad (64)$$

Beyond this simple situation, we often need to compute the trace of product operators multiplied with a permutation operator, i.e. an expression of the form $\text{tr}(A_1 \otimes A_2 \otimes \dots \otimes A_k R_\sigma)$. Here, we can follow the same arguments as above: First, if $\sigma = \gamma = (k, k-1, \dots, 1)$ is the cyclic permutation, then

$$\text{tr}(A_1 \otimes A_2 \otimes \dots \otimes A_k R_\gamma) = \sum_{x_1, \dots, x_k} \langle x_1, \dots, x_k | A_1 \otimes A_2 \otimes \dots \otimes A_k | x_2, x_3, \dots, x_k, x_1 \rangle \quad (65)$$

$$= \sum_{x_1, \dots, x_k} (A_1)_{x_1, x_2} (A_2)_{x_2, x_3} \dots (A_k)_{x_k, x_1} = \text{tr}(A_1 A_2 \dots A_k). \quad (66)$$

For a general permutation, the Kronecker deltas connect indices along each cycle independently. If $\sigma = (a_1 a_2 \dots a_\ell)$ is one cycle, our convention Eq. (53) gives

$$\text{tr}[(A_1 \otimes \dots \otimes A_k) R_\sigma] \longrightarrow \sum_{x_{a_1}, \dots, x_{a_\ell}} (A_{a_1})_{x_{a_1}, x_{a_\ell}} (A_{a_2})_{x_{a_2}, x_{a_1}} \dots (A_{a_\ell})_{x_{a_\ell}, x_{a_{\ell-1}}} \quad (67)$$

$$= \text{tr}(A_{a_1} A_{a_\ell} \dots A_{a_2}). \quad (68)$$

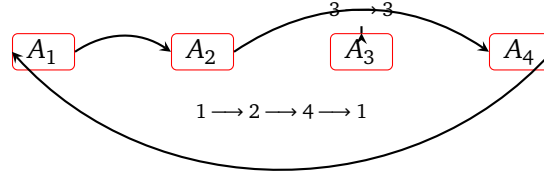


Figure 2: Cycle-trace contraction for $\sigma = (1\ 4\ 2)(3)$. Following an arrow follows a contracted matrix index. The three-cycle produces one trace, in the order fixed by Eq. (53); the fixed point produces a separate trace.

Different cycles use disjoint summation indices, so their contributions multiply. Thus, if $\mathcal{C}(\sigma)$ denotes the set of cycles,

$$\text{tr}[(A_1 \otimes \cdots \otimes A_k)R_\sigma] = \prod_{(a_1 \dots a_\ell) \in \mathcal{C}(\sigma)} \text{tr}(A_{a_1} A_{a_\ell} \cdots A_{a_2}). \quad (69)$$

The apparent reversal inside each trace is only a consequence of our explicit permutation convention. It disappears when all factors are equal.

A cycle contraction with a non-trivial order. Take $\sigma = (1\ 4\ 2)(3)$. Since $\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 3$, and $\sigma^{-1}(4) = 1$, the convention in Eq. (53) gives

$$\begin{aligned} & \text{tr}[(A_1 \otimes A_2 \otimes A_3 \otimes A_4)R_\sigma] \\ &= \sum_{x_1, \dots, x_4} (A_1)_{x_1 x_2} (A_2)_{x_2 x_4} (A_3)_{x_3 x_3} (A_4)_{x_4 x_1} \\ &= \left[\sum_{x_1, x_2, x_4} (A_1)_{x_1 x_2} (A_2)_{x_2 x_4} (A_4)_{x_4 x_1} \right] \left[\sum_{x_3} (A_3)_{x_3 x_3} \right] \\ &= \text{tr}(A_1 A_2 A_4) \text{tr}(A_3). \end{aligned} \quad (70)$$

The arrows in Fig. 2 are therefore not an extra rule: they are a compact record of the Kronecker-index contractions. In particular, the order $A_1 A_2 A_4$ is fixed by the chosen action of R_σ , rather than by an arbitrary reading order of the cycle notation. For the important case when $A_1 = A_2 = \cdots = A_k =: A$, the final result is simplified to

$$\text{tr}(A^{\otimes k} R_\sigma) = \prod_{\ell \in \lambda(\sigma)} \text{tr}(A^\ell), \quad (71)$$

where $\lambda(\sigma)$ is the multiset of cycle lengths of σ .

Symmetric subspace Throughout this course, symmetries under permutations will play a fundamental role, in particular the subspace of $(\mathbb{C}^d)^{\otimes k}$ composed of vectors that are left invariant by permutations:

$$\text{Sym}_{k,d} \equiv \text{Sym}((\mathbb{C}^d)^{\otimes k}) := \{\psi \in (\mathbb{C}^d)^{\otimes k} \mid R_\sigma |\psi\rangle = |\psi\rangle \ \forall \sigma \in S_k\}. \quad (72)$$

We will now show that the projector onto $\text{Sym}_{k,d}$ is

$$P_{\text{Sym},k,d} = \frac{1}{k!} \sum_{\sigma \in S_k} R_\sigma. \quad (73)$$

To see this, we first check that $P_{\text{Sym},k,d}$ is an orthogonal projector:

$$P_{\text{Sym},k,d}^2 = \frac{1}{(k!)^2} \sum_{\sigma, \pi \in S_k} R_{\sigma\pi} = \frac{1}{k!} \sum_{\sigma \in S_k} \frac{1}{k!} \sum_{\tau \in S_k} R_{\tau} = P_{\text{Sym},k,d}, \quad (74)$$

$$P_{\text{Sym},k,d}^\dagger = \frac{1}{k!} \sum_{\sigma \in S_k} R_{\sigma^{-1}} = \frac{1}{k!} \sum_{\pi \in S_k} R_{\pi} = P_{\text{Sym},k,d}, \quad (75)$$

where we substituted variables as $\tau = \sigma\pi$ and $\pi = \sigma^{-1}$, respectively, and used that the sum is invariant under the change of variables. Next, note that for all $\psi \in \text{Sym}_{k,d}$:

$$P_{\text{Sym},k,d}|\psi\rangle = \frac{1}{k!} \sum_{\sigma \in S_k} R_{\sigma}|\psi\rangle = \frac{1}{k!} \sum_{\sigma \in S_k} |\psi\rangle = |\psi\rangle, \quad (76)$$

thus, $\text{Sym}_{k,d}$ is in the range of $P_{\text{Sym},k,d}$. Moreover, if $P_{\text{Sym},k,d}|\psi\rangle = |\psi\rangle$, then

$$R_{\pi}|\psi\rangle = R_{\pi}P_{\text{Sym},k,d}|\psi\rangle = \frac{1}{k!} \sum_{\sigma \in S_k} R_{\pi\sigma}|\psi\rangle = \frac{1}{k!} \sum_{\tau \in S_k} R_{\tau}|\psi\rangle = P_{\text{Sym},k,d}|\psi\rangle = |\psi\rangle, \quad (77)$$

and thus the range of $P_{\text{Sym},k,d}$ is exactly $\text{Sym}_{k,d}$. We can now compute the dimension of the symmetric subspace using Eq. (64) and Ex. 2.4 as

$$\begin{aligned} \dim \text{Sym}_{k,d} &= \text{tr } P_{\text{Sym},k,d} = \frac{1}{k!} \sum_{\sigma \in S_k} d^{\#\sigma} \\ &= \frac{1}{k!} \sum_{r=1}^k c(k,r) d^r = \frac{d(d+1)\cdots(d+k-1)}{k!} \\ &= \binom{d+k-1}{k}. \end{aligned} \quad (78)$$

Graphical representation While the above methodologies are generic and straightforward, the algebra is often cumbersome. For this reason, it is useful to introduce a graphical notation to represent permutations. Similar to the Feynman diagrammatics for perturbative expansions, this is simply a bookkeeping of the operation previously described.

We draw a permutation by connecting input position j to output position $\sigma(j)$. For example, the five-element permutation $\tau = (12)(35)(4)$ is represented by

$$\begin{array}{c} 1 \text{ --- } \diagup \text{ --- } 3 \\ 2 \text{ --- } \diagdown \text{ --- } 4 \\ (12)(35)(4) \cong 3 \text{ --- } \diagup \text{ --- } 5 \\ 4 \text{ --- } \diagdown \text{ --- } 1 \\ 5 \text{ --- } \text{ --- } 2 \end{array} \quad (79)$$

This notation is particularly useful, since it makes computing products particularly easy. In the next diagram the lines for $\sigma = (123)(4)(5)$ are encountered first and those for $\tau = (12)(35)(4)$

second; it therefore represents $\tau \cdot \sigma$:

$$\tau \cdot \sigma \cong \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \\ \diagup \end{array} \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \cong \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \diagup \\ \diagdown \\ \diagup \\ \diagdown \\ \diagup \end{array} \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \cong (235)(1)(4) \quad (80)$$

Since the group structure is the same for the representations of S_k , we can use the same notation also for the operators $\{R_\sigma : \sigma \in S_k\}$. For representations, the diagrammatic notation allows also to include traces and product by operators: Taking a trace requires adding curves that connect the initial and final endpoints. For example:

$$\text{tr}(R_\sigma) = \begin{array}{c} \text{diagram of } R_\sigma \text{ with trace} \end{array} = (\bigcirc)^{\#(\sigma)} = d^{\#(\sigma)}. \quad (81)$$

Similarly, for operators we have

$$\text{tr}(A^{\otimes k} R_\sigma) = \begin{array}{c} \text{diagram of } A^{\otimes k} R_\sigma \text{ with trace} \end{array} = \text{tr}(A^3) \text{tr}(A)^2 \quad (82)$$

2.3 Weingarten calculus

As noted in Section 2.1, $M_k(A)$ lies in the unitary commutant and can thus be written as a linear combination

$$M_k(A) = \sum_{\pi \in S_k} c_\pi(A) R_\pi, \quad (83)$$

for some coefficients $c_\pi(A)$. A natural question to ask is whether these coefficients are unique, i.e. whether permutations form a basis for the commutant. Intriguingly, this is the case if the dimension d is large enough:

Lemma 2.2. *The set $\{R_\sigma \mid \sigma \in S_k\}$ is linearly independent for $d \geq k$.*

Proof. We consider the standard basis of $\mathbb{C}^d$, which we here denote as $|1\rangle, \dots, |d\rangle$. Since $k \leq d$, we can consider the action of permutations on $|1, \dots, k\rangle \in (\mathbb{C}^d)^{\otimes k}$:

$$R_\pi |1, \dots, k\rangle = |\pi^{-1}(1), \dots, \pi^{-1}(k)\rangle. \quad (84)$$

Suppose that $\sum_{\pi \in S_k} c_\pi R_\pi = 0$. Applying this operator to $|1, \dots, k\rangle$ gives

$$\sum_{\pi} c_\pi |\pi^{-1}(1), \dots, \pi^{-1}(k)\rangle = 0. \quad (85)$$