

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

A.1	Unsigned Stirling numbers of the first kind	92
A.2	States, operators, superoperators	92
A.3	Non-orthonormal bases	97

1 About this course

Quantum information asks how information is represented, processed, and transmitted when the underlying degrees of freedom obey quantum mechanics. Many-body physics asks how simple microscopic rules produce collective behaviour in systems with many interacting components. The two subjects meet because entanglement, scrambling, and computational resources are properties of an entire quantum state rather than of a single local observable.

Programmable quantum devices make this connection operational. They can prepare phases whose useful structure is described by entanglement, nonstabilizerness (“magic”), or error-correcting properties, even when no conventional local order parameter is available. At the same time, the Hilbert-space dimension grows exponentially with system size, so direct calculations quickly become impossible. Random unitaries, random circuits, and tensor-network representations provide controlled models in which one can compute ensemble averages and identify behaviour that is typical rather than fine-tuned.

These notes develop that toolbox from first principles and then use it for state estimation, anticoncentration, magic, entanglement growth, and operator scrambling. The presentation is intended for Master’s students. We assume a first course in quantum mechanics and the elementary linear algebra and analysis normally covered in first-year mathematics courses; representation theory, probability on groups, concentration inequalities, and tensor-network methods are introduced when they first become necessary.

1.1 How to use these notes

Every new mathematical object is introduced in three stages: first the question it answers, then a precise definition, and finally a worked example or derivation. Starred sections contain useful extensions but are not needed for a first reading. Each main section ends with exercises arranged roughly from foundational to advanced. A separate companion volume contains complete solutions, including intermediate algebraic steps.

The logical route is as follows.

- Sec. 2: *Quantum Randomness I* introduces Haar measure, permutations, Weingarten calculus, unitary designs, and the Clifford group.
- Sec. 3: *Classical Shadows* turns randomized measurements into unbiased estimators and derives their sample complexity.
- Sec. 4: *Quantum Randomness II* replaces global Haar unitaries by finite-depth random circuits and relates convergence to moment-operator spectral gaps.
- Sec. 5: *Random Dynamics in Many-Body Systems* applies the preceding tools to anticoncentration, Pauli spectra and magic, entanglement growth, and out-of-time-order correlators.

1.2 Global notation

The following conventions are used throughout. Subscripts indicate a subsystem only when this is stated explicitly; otherwise they are ordinary indices.

Symbol	Meaning
$\mathcal{H} = (\mathbb{C}^q)^{\otimes n}$	Hilbert space of n qudits of local dimension q ; its total dimension is $d = q^n$.
k	Moment or replica order. The symmetric group on k objects is S_k .
A, B	Operators by default; when a bipartition is declared, subsystem labels with Hilbert-space dimensions d_A and d_B .
$\mathbb{1}_X$	Identity operator on subsystem or space X ; the subscript is omitted when unambiguous.
$F = R_{(12)}$	Two-copy swap operator; it exchanges the two replica factors.
tr_X	Partial trace over X ; tr without a subscript is the full trace.
$\mathbb{E}_{U \sim \mu}[\cdot]$	Expectation for a random unitary sampled from the measure μ ; Haar measure is normalized to one.
R_π	Operator representing the permutation $\pi \in S_k$ on $\mathcal{H}^{\otimes k}$.
$\ X\ _p$	Schatten p -norm; in particular $p = 1, 2, \infty$ give the trace, Hilbert–Schmidt, and operator norms.

All logarithms are natural unless a base is displayed explicitly. Therefore entropies are measured in nats; divide by $\log 2$ to obtain bits. We reserve d for differentials, as in $d\mu(U)$, and d for the total Hilbert space dimension.

2 Quantum Randomness I

This section gives a precise meaning to a “uniformly random” unitary and develops a practical calculus for its moments. Haar invariance reduces the integral to a symmetry problem; permutations describe the relevant symmetry sector; and the inverse Gram matrix supplies the coefficients through Weingarten calculus. Unitary designs and the Clifford group then show how much of Haar randomness can be reproduced without implementing a generic unitary.

2.1 What is a Haar measure?

Lebesgue measure on $\mathbb{R}$ is translation invariant: shifting a set does not change its length. Because $\mathbb{R}$ is non-compact, however, its total length is infinite, so there is no translation-invariant probability distribution on the whole real line. Compact groups avoid this obstruction.

Theorem 2.1 (Normalized Haar measure). *Let G be a compact Hausdorff topological group. There is a unique normalized regular Borel measure μ_G such that, for every integrable function f and every fixed $h \in G$,*

$$\int_G f(g) d\mu_G(g) = \int_G f(hg) d\mu_G(g) = \int_G f(gh) d\mu_G(g), \quad \int_G d\mu_G(g) = 1. \quad (1)$$

It is called the normalized Haar measure on G .

The unitary group $U(d)$ is compact. We abbreviate its normalized Haar measure by dU and write

$$\int_{U(d)} f(U) dU = \int_{U(d)} f(VU) dU = \int_{U(d)} f(UV) dU \quad \text{for every fixed } V \in U(d). \quad (2)$$

Thus “uniform” means invariant under a change of origin in the group, not that one has assigned an equal positive probability to each of infinitely many matrices. We write $U \sim \text{Haar}(U(d))$ when U is sampled from this measure.

The action of $U(d)$ on normalized state vectors is transitive: given $|\psi\rangle$ and $|\varphi\rangle$, extend each vector to an orthonormal basis and map the first basis to the second. The resulting unitary satisfies $U|\psi\rangle = |\varphi\rangle$. Consequently $U|0\rangle$, with Haar-random U , defines the unitarily invariant distribution on pure states. We call its samples *Haar-random states*.

Haar integrals and moments. Let f be a function of a unitary. Its ensemble average is

$$\mathbb{E}_{U \sim \text{Haar}(U(d))}[f(U)] := \int_{U(d)} f(U) dU. \quad (3)$$

For example, prepare $|\psi\rangle$, apply U , and measure in the basis $\{|i\rangle\}_{i=0}^{d-1}$. The Born probability of outcome i is $p_U(i) = |\langle i|U|\psi\rangle|^2$. The first Haar twirl, derived below, gives

$$\mathbb{E}_U[p_U(i)] = \text{tr}[|i\rangle\langle i| \mathbb{E}_U(U|\psi\rangle\langle\psi|U^\dagger)] = \text{tr}\left(|i\rangle\langle i| \frac{\mathbb{1}}{d}\right) = \frac{1}{d}. \quad (4)$$

This statement fixes only the mean. Fluctuations require the second moment:

$$\text{Var}_U[p_U(i)] = \mathbb{E}_U[p_U(i)^2] - \frac{1}{d^2}, \quad (5)$$

$$p_U(i)^2 = \text{tr}[|i\rangle\langle i|^{\otimes 2} U^{\otimes 2} |\psi\rangle\langle\psi|^{\otimes 2} (U^\dagger)^{\otimes 2}]. \quad (6)$$

We will find $\text{Var}_U[p_U(i)] = (d-1)/(d^2(d+1))$ and return to its physical interpretation in section 5.1.

A second example is the purity of a subsystem. Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, $\rho = U|\psi\rangle\langle\psi|U^\dagger$, and $\rho_A = \text{tr}_B \rho$. On two copies, let F_A exchange the two A factors and act trivially on the two B factors. The *swap trick* states that

$$\text{tr}(\rho_A^2) = \text{tr}[(\rho \otimes \rho)(F_A \otimes \mathbb{1}_{BB'})]. \quad (7)$$

To see it without diagrammatic notation, choose product bases and expand

$$\text{tr}(\rho_A^2) = \sum_{a,a',b,b'} \rho_{ab,a'b} \rho_{a'b',ab'}, \quad (8)$$

which is exactly the index contraction on the right-hand side of eq. (7). Hence purity, although nonlinear in one copy of ρ , is a linear observable on two copies.

Both examples are *balanced polynomials*: every term contains the same number k of matrix entries of U and complex-conjugated entries of U . Every balanced polynomial of bidegree (k, k) is a linear combination of matrix elements of

$$p_{A,B}(U) := \text{tr}[B U^{\otimes k} A (U^\dagger)^{\otimes k}], \quad (9)$$

where $A, B \in L(\mathcal{H}^{\otimes k})$. This motivates the k th Haar twirl

$$M_k(A) := \int_{U(d)} U^{\otimes k} A (U^\dagger)^{\otimes k} dU. \quad (10)$$

If A is a k -copy state and B an observable, then $\text{tr}[B M_k(A)]$ is the ensemble-averaged expectation value obtained by applying the same random unitary to every copy. The task of this section is to evaluate eq. (10) without introducing coordinates on $U(d)$.

Example 2.1: Computing a Haar integral in coordinates

Consider $d = 2$ and the first moment

$$\int_{U(2)} UAU^\dagger dU \quad \text{for } A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}. \quad (11)$$

The global phase cancels in $UAU^\dagger$, so it is enough to parametrize $SU(2)$ as

$$U(\theta, \alpha, \beta) = \begin{pmatrix} e^{i\alpha} \cos \theta & e^{i\beta} \sin \theta \\ -e^{-i\beta} \sin \theta & e^{-i\alpha} \cos \theta \end{pmatrix} \quad (12)$$

with $0 \leq \theta \leq \pi/2$ and $0 \leq \alpha, \beta < 2\pi$. The normalized measure is

$$dU = \frac{\sin(2\theta)}{4\pi^2} d\theta d\alpha d\beta. \quad (13)$$

For the upper-left entry,

$$(UAU^\dagger)_{11} = \cos^2 \theta a_{11} + \sin^2 \theta a_{22} + \sin \theta \cos \theta (e^{i(\alpha-\beta)} a_{12} + e^{-i(\alpha-\beta)} a_{21}). \quad (14)$$

The phase integrals kill the last two terms. The two remaining polar integrals are equal:

$$\int_0^{\pi/2} \sin(2\theta) \cos^2 \theta d\theta = \int_0^{\pi/2} \sin(2\theta) \sin^2 \theta d\theta = \frac{1}{2}. \quad (15)$$

The off-diagonal entries vanish by the same phase average. Therefore

$$\int_{U(2)} UAU^\dagger dU = \frac{\text{tr}(A)}{2} \mathbb{1}. \quad (16)$$

The calculation is elementary for $d = 2$ and $k = 1$, but coordinates become unwieldy as either parameter grows. The symmetry argument below scales much better.

The unitary commutant. The key observation in evaluating the integral (10) is that $M_k(A)$ commutes with all unitaries $U^{\otimes k}$ for $U \in U(d)$. The subspace of operators that commute with all $U^{\otimes k}$ is called the $(k\text{-fold})$ commutant of $U(d)$:

$$\text{Comm}_k = \{A \in L(\mathcal{H}^{\otimes k}) \mid U^{\otimes k} A = A U^{\otimes k} \forall U \in U(d)\}. \quad (17)$$

We then show the following lemma:

Lemma 2.1. $M_k(A) \in \text{Comm}_k$ for all $A \in L(\mathcal{H}^{\otimes k})$. In fact, every element in Comm_k is of the form $M_k(A)$.

Proof. Clearly, if A commutes with all $U^{\otimes k}$, then $M_k(A) = A$, i.e. every element in Comm_k is of the form $M_k(A)$. Vice versa, if $B = M_k(A)$, then, by the invariance of the Haar measure:

$$U^{\otimes k} B U^{\otimes k, \dagger} = \int_{U(d)} (UV)^{\otimes k} A (UV)^{\otimes k, \dagger} dV = \int_{U(d)} V^{\otimes k} A V^{\otimes k, \dagger} dV = B, \quad \forall U \in U(d). \quad (18)$$

Thus, $B \in \text{Comm}_k$. □

A central step in understanding the commutant is to realize that every $U^{\otimes k}$ commutes with any operator R_π that permutes the k copies of our Hilbert space $\mathcal{H}$ according to the

permutation π . For instance, $U^{\otimes 2}$ clearly commutes with a swap of the two copies. Hence, the permutation operators R_π are contained in the k -th fold unitary commutant. These permutation operators form what is called a *representation* of the *symmetric group* S_k . A powerful result from representation theory – the *Schur-Weyl duality* – then tells us that the groups $U(d)$ and S_k are *dual to each other* which, among others, implies that every element in the commutant Comm_k can be written as a linear combination of permutation operators R_π :

Theorem 2.2 (Schur-Weyl duality). *The k -fold unitary commutant Comm_k is spanned by $\{R_\sigma \mid \sigma \in S_k\}$. Vice versa, the commutant of $\{R_\sigma \mid \sigma \in S_k\}$ is spanned by $\{U^{\otimes k} \mid U \in U(d)\}$*

We will not seek a deeper understanding of Schur-Weyl duality in this course but merely take this result as a motivation to develop techniques to evaluate $M_k(A)$. In particular, Schur-Weyl duality allows us to express $M_k(A)$ as a linear combination over permutations, with coefficients determined by their combinatorics. This leads to the framework known as *Weingarten calculus*, which enables the exact evaluation of many relevant integrals over the unitary group. As a result, permutations will play a key role throughout this course – not for abstract mathematical reasons, but because they offer a concrete and computable handle on random quantum processes.

2.2 Permutations and their combinatorics

In this section, we will introduce the essential properties of permutations needed for our purposes. While there is a rich and beautiful mathematical structure behind these ideas, we will focus only on the aspects that are directly relevant for our discussion and applications.

2.2.1 Permutations and Cycles

A *permutation* is a reordering of a finite set of elements. In this course, we consider permutations of the set $\{1, 2, \dots, k\}$. We will denote permutations by Greek letters such as π, σ, τ , and so on. The set of all permutations of k elements forms a group under composition, called the *symmetric group*, and denoted by S_k .

Given a permutation $\sigma \in S_k$ and an element $x \in \{1, \dots, k\}$, we write $\sigma(x)$ to indicate the image of x under σ . A common and explicit way to write a permutation is the *two-line notation*, where the first row lists the original elements and the second row gives their images under the permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma(1) & \sigma(2) & \dots & \sigma(k) \end{pmatrix}. \quad (19)$$

Example 2.2: Explicit Notation of Permutations

An example of a permutation of four elements is:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}. \quad (20)$$

This means that the permutation acts as:

$$\sigma(1) = 3, \quad \sigma(2) = 1, \quad \sigma(3) = 4, \quad \sigma(4) = 2. \quad (21)$$

The group operation in S_k is the composition of permutations, denoted by $\sigma \cdot \tau$ for $\sigma, \tau \in S_k$, and defined by

$$(\sigma \cdot \tau)(x) = \sigma(\tau(x)) \quad \text{for all } x \in \{1, \dots, k\}. \quad (22)$$

Note that permutation composition is applied from right to left: τ acts first, followed by σ .