Quantum Information Methods for Many-Body Physics

Xhek Turkeshi Markus Heinrich

Institute for Theoretical Physics, University of Cologne

April 8, 2025

CONTENTS

1	Introduction	2
	1.1 Overview Overview 1.2 Permutations and their combinatorics Overview	2 3
	1.2.1 Permutations and Cycles	3
	1.2.2 The Action of Permutations on Quantum States 1.3 Further reading	8 12
2	Ouantum Randomness I	13
	2.1 What is a Haar measure?	13
	2.2 Haar integration and Weingarten calculus	13
	2.2.1 The unitary commutant	14
	2.2.2 Weingarten calculus	15
	2.3 Approximating the Haar measure: Unitary designs	18
	2.4 Further reading	18
3	Measuring Properties of Many-Body States	19
	3.1 Shadow estimation: Expectation values through randomized measurements	19
	3.2 Applications	19
4	Quantum Randomness II	20
-	4.1 Random quantum circuits	20
=	Random Dynamics in Many Rody Systems	01
3	5.1 Entanglement dynamics and membrane picture	21
	5.2 Ouantum scrambling in chaotic systems	21
Α	Some linear algebra	22
	A.1 States, operators, superoperators	22
	A.2 Non-orthonormal bases	- 24

INTRODUCTION

Quantum information science is the field that studies how information is stored, processed, and transmitted when it is governed by the laws of quantum mechanics. It includes areas such as *quantum computing*, *quantum communication*, *quantum cryptography*, *quantum sensing*, *and quantum error correction*. Although still relatively young, quantum information science has already had a profound impact on many areas of physics, especially on the study of quantum systems composed of many interacting *particles*, commonly referred to as *many-body quantum systems*.

Within this context, *quantum circuits* and *tensor networks* have emerged as essential tools to tackle fundamental questions in quantum dynamics—from the mechanisms of *thermalization* and the emergence of *statistical mechanics* in isolated systems, to the onset of *quantum chaos* and its deep connections with *black hole physics and holography* in quantum gravity. Studying these phenomena in a concrete setting is notoriously difficult, due to the exponential growth of the Hilbert space and the inherently non-linear structure of quantum correlations. *Random quantum circuits* and *tensor networks* offer a powerful way to overcome these challenges: they enable analytical and numerical progress through disorder averaging, while capturing the typical behavior of generic quantum systems thanks to *quantum typicality arguments*.

Crucially, the interplay between quantum information and many-body physics has not only refined our understanding of traditional problems, but has also uncovered entirely new dynamical phases of matter – phases that arise uniquely in *programmable quantum devices*. This so-called *synthetic quantum matter* cannot be characterized by conventional local order parameters such as magnetization or current. Instead, its defining features are quantum informational, such as the structure of entanglement or nonstabilizer (magic state) resources, or the system's ability to preserve quantum information against noise and local errors. Understanding and classifying such phases requires a shift in perspective –from symmetry and energetics to *information content* and *computational complexity*.

At the same time, random unitary dynamics, especially in the form of random quantum circuits, have become indispensable tools in the *NISQ (noisy intermediate-scale quantum)* era. They provide efficient and versatile frameworks for a wide range of applications, including the benchmarking and verification of quantum computations, the characterization of noise in experimental platforms, and the estimation of observables via shadow tomography. Far from being purely theoretical constructs, these methods are implemented across various platforms – from superconducting qubits to cold atoms – and are central to the ongoing development of near-term quantum technologies.

This course provides a pedagogical introduction to random unitaries and to several key methods from quantum information theory, with a focus on their application to many-body physics. A substantial part of the course covers research-level topics introduced only in the past few years, offering a unique opportunity to engage with current questions at the interface between two rapidly evolving fields. It is also intended to serve as a solid preparation to pursue a Master's thesis, a doctorate or work in the private for these areas.

1.1 Overview

The structure of the course is as follows. We begin with a chapter on permutations and a graphical calculus, which will provide the foundation for the treatment of randomization methods throughout the course. We then introduce the core randomization concepts in two parts, Quantum Randomness I and II—each followed by a chapter that connects the methods to applications in many-body systems.

1. In Quantum Randomness I (Ch. 2), we introduce *Weingarten calculus*, the central toolbox for computing averages over the unitary group, which naturally arise when considering statistical

properties of random evolutions. We also *study unitary designs*, which provide efficient approximations of Haar randomness and play an important role in practical implementations.

- 2. In Ch. 3, we present the *framework of classical shadows*. Introduced around 2020, classical shadows offer an efficient way to extract information about quantum states using only a small number of randomized measurements. This technique has already found widespread use in experimental platforms and continues to inspire a growing body of research.
- 3. In Quantum Randomness II (Ch. 4), we explore random quantum circuits in detail. These models provide an efficient and physically motivated approach to generate randomness in quantum many-body systems, and they serve as minimal models for chaotic quantum dynamics.
- 4. In Ch. 5, we show how random circuits can be used to model scrambling, thermalization, and information spreading in interacting quantum systems. These models also offer connections to quantum chaos, complexity growth, and typicality in many-body physics.

Each chapter concludes with a short guide to the research literature, primarily in the form of original articles, allowing students to explore further and connect the course material to current work in the field.

1.2 Permutations and their combinatorics

Why permutations? A central theme of this course is the study of random unitaries and their applications in quantum many-body systems. To understand their behavior, we need to analyze the statistics of random unitaries—specifically, we are interested in computing averages, variances, and higher moments of functions involving random unitary matrices.

At first glance, this might seem daunting: computing integrals over the unitary group is, in general, a highly nontrivial task. However, a powerful insight from representation theory, known as *Schur-Weyl duality*, provides a way forward. This duality reveals a deep connection *between the action of the unitary group and the action of the permutation group*, which allows us to reformulate complicated integrals in terms of combinatorics of permutations.

This leads to the framework known as *Weingarten calculus*, which enables the exact evaluation of many relevant averages 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.

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. The interested reader can consult the bibliography.

1.2.1 Permutations and Cycles

A *permutation* is a reordering of a finite set of elements. In this course, we consider permutations of the set $\{1, 2, ..., k\}$. 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 $x \in \{1, ..., k\}$, 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:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma(1) & \sigma(2) & \dots & \sigma(k) \end{pmatrix}.$$
 (1.1)

Example 1.2.1: Explicit Notation of Permutations

An example of a permutation of four elements is:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$
 (1.2)

This means that the permutation acts as:

$$\sigma(1) = 3, \quad \sigma(2) = 1, \quad \sigma(3) = 4, \quad \sigma(4) = 2.$$
 (1.3)

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

$$(\sigma \cdot \tau)(x) = \sigma(\tau(x)) \quad \text{for all } x \in \{1, \dots, k\}.$$
(1.4)

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

Example 1.2.2: Product of Permutations

Consider the following two permutations of k = 4 elements:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$
 (1.5)

To compute the composition $(\tau \cdot \sigma)(x) = \tau(\sigma(x))$, we apply σ first and then τ :

$$\begin{aligned}
\sigma(1) &= 3, \quad \tau(\sigma(1)) = \tau(3) = 3, \\
\sigma(2) &= 1, \quad \tau(\sigma(2)) = \tau(1) = 4, \\
\sigma(3) &= 4, \quad \tau(\sigma(3)) = \tau(4) = 1, \\
\sigma(4) &= 2, \quad \tau(\sigma(4)) = \tau(2) = 2.
\end{aligned}$$
(1.6)

Putting everything together, we find:

$$\tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$
 (1.7)

It is important to emphasize that for $k \ge 3$, the symmetric group S_k is *non-abelian*, meaning that the order of composition matters – in general, $\sigma \cdot \tau \ne \tau \cdot \sigma$.

Exercise 1.1. Consider the permutations from Example 1.2.2. Compute the product $\sigma \cdot \tau$, and verify that it differs from $\tau \cdot \sigma$.

The symmetric group contains a special element called the *identity permutation*, denoted by ι , which leaves all elements unchanged:

$$\iota = \begin{pmatrix} 1 & 2 & \dots & k \\ 1 & 2 & \dots & k \end{pmatrix}. \tag{1.8}$$

By definition, composition with the identity does not change the permutation:

$$\iota \cdot \sigma = \sigma = \sigma \cdot \iota. \tag{1.9}$$

Moreover, every permutation $\sigma \in S_k$ has an *inverse* σ^{-1} such that:

$$\sigma \cdot \sigma^{-1} = \iota = \sigma^{-1} \cdot \sigma. \tag{1.10}$$

To compute the inverse of a permutation π , for each index $i \in \{1, 2, ..., k\}$ we set $\pi^{-1}(\pi(i)) = \iota(i) = i$. The resulting list π^{-1} is the inverse permutation.

Example 1.2.3: Inverse of a Permutation

Consider the following two permutations of k = 5 elements:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}.$$
 (1.11)

To compute the inverse σ^{-1} we use the rule $\sigma^{-1}(\sigma(i)) \equiv i$

$$\sigma(1) = 3 \Rightarrow \sigma^{-1}(3) = 1$$

$$\sigma(2) = 5 \Rightarrow \sigma^{-1}(5) = 2$$

$$\sigma(3) = 1 \Rightarrow \sigma^{-1}(1) = 3$$

$$\sigma(4) = 2 \Rightarrow \sigma^{-1}(2) = 4$$

$$\sigma(5) = 4 \Rightarrow \sigma^{-1}(4) = 5$$

(1.12)

Reordering the list in terms of the argument, we find

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$
 (1.13)

A *cyclic permutation*, or simply a *cycle*, is a specific type of permutation in which a subset of elements is permuted in a closed loop, while all remaining elements remain fixed. Formally, an *l*-cycle is a permutation that permutes *r* elements cyclically and leaves the other k - l elements unchanged. The number *l* is called the *length of the cycle*.

Concretely, a cycle of length *l* means that there exists a subset $\{i_1, i_2, ..., i_l\} \subset \{1, 2, ..., k\}$ such that

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots, \quad \sigma(i_{l-1}) = i_l, \quad \sigma(i_l) = i_1, \tag{1.14}$$

and for all other elements $x \notin \{i_1, \ldots, i_l\}$, we have $\sigma(x) = x$.

Exercise 1.2 (Cyclic permutations). *The following are examples of cyclic permutations:*

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}.$$
 (1.15)

Can you identify the subset $\{a_1, ..., a_l\}$ *that is cyclically permuted in each case? What is the length l of each cycle?* [Answer: For τ , r = l; for σ , r = l.]

One fundamental property of cycles is that any permutation can be decomposed into a product of disjoint cycles. That is, for any $\sigma \in S_k$, there exists a unique set of cycles that act on mutually disjoint subsets of $\{1, 2, ..., k\}$. This decomposition is unique up to the order in which the cycles are written. This motivates the *cycle notation* of permutations:

$$\sigma = (a_1 a_2 \dots a_{j_1})(a_{j_1+1} a_{j_1+2} \dots a_{j_2}) \dots (a_{j_{r-1}+1} a_{j_{r-1}+2} \dots a_{j_r}).$$
(1.16)

Here, each tuple represents a cycle, and all elements a_m are drawn from $\{1, 2, ..., k\}$ without repetition. The integer $r = \#(\sigma)$ denotes the *number of disjoint cycles* in the decomposition of σ .

Let us now describe an explicit algorithm to obtain the cycle decomposition of a permutation, as in Eq. (1.16). The idea is simple: we iteratively follow the action of the permutation until we return to the starting point, keeping track of all visited elements.

(i) Start from the smallest unvisited element. Initially, this is x = 1. If 1 has already been included in a previous cycle, move to the next smallest unvisited element.

(ii) **Construct a cycle by iterating the permutation.** Begin by writing down *x*. Then repeatedly apply the permutation π to generate the sequence

 $x, \pi(x), \pi(\pi(x)), \pi(\pi(\pi(x))), \ldots$

Continue this process until you return to the starting point *x*. The list of elements

$$(x \ \pi(x) \ \pi^2(x) \ \dots \ \pi^{j-1}(x))$$
 (1.17)

forms a cycle of length *j*. Mark all of these elements as visited.

(iii) **Repeat the process.** Find the next smallest unvisited element and return to step (ii). Continue until all elements have been visited. The full cycle decomposition of π is then obtained by combining the individual cycles found in each iteration.

Example 1.2.4: Cycle decomposition

Consider the permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$
 (1.18)

We apply the cycle decomposition algorithm step by step:

• Start with 1:

$$1 \stackrel{\tau}{\mapsto} 4 \stackrel{\tau}{\mapsto} 1.$$

This gives the first cycle: (1 4). Mark 1 and 4 as visited.

• Next smallest unvisited element is 2:

 $2 \xrightarrow{\tau} 5 \xrightarrow{\tau} 2.$

This gives the second cycle: (2 5). Mark 2 and 5 as visited.

• The last unvisited element is 3, and since

 $3 \stackrel{\tau}{\mapsto} 3$,

this is a fixed point (a 1-cycle), written as (3).

Combining the above, the full cycle decomposition is:

 $\tau = (1\ 4)(2\ 5)(3). \tag{1.19}$

Note that the *order* in which disjoint cycles are written is irrelevant. For instance, in Example 1.2.4, all of the following represent the same permutation:

$$\tau = (1 4)(2 5)(3) = (2 5)(1 4)(3) = (3)(1 4)(2 5).$$

When the total number of elements *k* is clear from the context (e.g., k = 5 in this case), it is common to omit one-cycles, also denoted *fixed points*, because these elements are understood to remain unchanged under the permutation. Using this convention, the permutation in Example 1.2.4 is simply written as:

$$\tau = (1\ 4)(2\ 5). \tag{1.20}$$

With this notation, the identity permutation is denoted by $\iota = ()$, which is shorthand for $\iota = (1)(2)\cdots(k)$ – that is, all elements are fixed.

The *cycle structure* of a permutation, denoted by $\lambda(\pi)$, is the list of the lengths of its disjoint cycles. For example, the permutation $\tau = (1 \ 4)(2 \ 5)$ has cycle structure $\lambda(\tau) = (2, 2, 1)$. The number of disjoint cycles is then given by the length of this list:

$$#(\pi) = |\lambda(\pi)|, \quad \text{for any } \pi \in S_k.$$
(1.21)

Example 1.2.5: Cycle Structure

Consider the following permutations of 6 elements

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 1 & 3 \end{pmatrix}.$$
 (1.22)

It is a simple exercise to show that their cycle decomposition is $\tau = (1,5,3)(2,4,6)$ and $\sigma = (1,5)(3,6)$ [which is a shorthand notation for $\sigma = (1,5)(3,6)(2)(4)$]. The permutation τ has two cycles of length 3, hence the cycle structure is $\lambda(\tau) = (3,3)$. Instead, σ is composed of two 2-cycles and two 1-cycles, so the cycle structure is $\lambda(\sigma) = (2,2,1,1)$.

Exercise 1.3. Show that conjugation preserves the cycle structure of a permutation. That is, for any σ , $\pi \in S_k$, prove that

$$\lambda(\pi\sigma\pi^{-1}) = \lambda(\sigma).$$

Transpositions, also known as *swaps*, are a special class of permutations that exchange exactly two elements and leave all others unchanged. A transposition has the form:

$$\sigma = (i j) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & k \\ 1 & \dots & j & \dots & i & \dots & k \end{pmatrix}.$$
 (1.23)

It is straightforward to verify that *any permutation* can be written as a product of transpositions. However, unlike the decomposition into disjoint cycles, this representation is *not unique* – a given permutation can be written in many different ways as a product of transpositions. While this makes the transposition decomposition less suitable for labeling permutations, it is extremely useful in algebraic manipulations. For instance, it turns out that the number of transpositions in any representation is always odd or always even, which justifies the definition of the *sign of a permutation*:

$$\operatorname{sgn}(\sigma) = (-1)^{\#\operatorname{transpositions in}\sigma}.$$
(1.24)

The sign function is important for the construction of representations of S_k and plays an important role in multilinear algebra, in particular in the definition of the *determinant of a matrix*.

We conclude this section by reviewing some structural aspects of the symmetric groups S_k for varying values of k. A key property is that the group S_k naturally embeds into S_{k+1} : that is, every permutation of k elements can be viewed as a permutation of k + 1 elements that leaves the (k + 1)-th element fixed. More formally, we can write

$$S_{k+1} = S_k \sqcup \{ (j k+1) \cdot \sigma : \sigma \in S_k, j = 1, 2, \dots, k \},$$
(1.25)

where the union is disjoint and the second term represents all permutations obtained by composing an element of S_k with a transposition that swaps k + 1 with one of the first k elements.

This recursive structure is useful for establishing many properties of permutations by induction on *k*. A simple but important example is the total number of elements in the symmetric group.

Theorem 1.1 (Counting of Permutations). *Given* $k \ge 1$, *the total number of permutations in* S_k *is*

$$|\mathbf{S}_k| = k!. \tag{1.26}$$

Proof. The total number of permutations is given by the factorial $k! = k(k-1)\cdots 2 \cdot 1$, with the convention that 0! = 1. To prove this, we use induction.

For k = 1, the symmetric group $S_1 = \{\iota\}$ consists only of the identity permutation, so $|S_1| = 1 = 1!$.

Assume now that $|S_k| = k!$ for some $k \ge 1$. From Eq. (1.25), the next symmetric group can be written as

$$S_{k+1} = S_k \sqcup \{ (j k+1) \cdot \sigma : \sigma \in S_k, j = 1, ..., k \}.$$
(1.27)

There are *k* possible values of *j*, and for each *j*, σ runs over all *k*! permutations in S_k. Hence,

$$|S_{k+1}| = |S_k| + k \cdot |S_k| = k! + k \cdot k! = (k+1) \cdot k! = (k+1)!.$$
(1.28)

This completes the proof by induction.

Consider now the following permutations of six elements:

$$\sigma_1 = (1\ 2\ 3)(5\ 6), \quad \sigma_2 = (2\ 4\ 6\ 1), \quad \sigma_3 = (1\ 2)(3\ 4)(5\ 6).$$
 (1.29)

While their cycle structures differ, all three permutations have exactly three disjoint cycles. This illustrates that simply counting the number of cycles is a coarser classification than specifying the full *cycle structure*.

In many computations throughout this course, we will be interested in the number of permutations in S_k with a fixed number of cycles $r = \#(\sigma)$. This quantity is given by the *unsigned Stirling numbers of the first kind*, denoted by c(k, r). These numbers satisfy the recursive relation:

$$c(k+1,r) = k \cdot c(k,r) + c(k,r-1), \tag{1.30}$$

which allows them to be computed inductively, without explicitly listing all permutations. These numbers form a triangle similar to Pascal's triangle and are tabulated up to k = 10 in the Appendix.

Starting with the base case k = 1, where $S_1 = \{()\}$, we find:

$$c(1,0) = 0, \qquad c(1,1) = 1.$$
 (1.31)

Using the recurrence, the next values for k = 2 are:

$$c(2,0) = 0,$$
 $c(2,1) = 1,$ $c(2,2) = 1.$ (1.32)

Exercise 1.4. Compute the values c(k, r) for $1 \le r \le k$ when k = 3 and k = 4. Verify that:

$$\sum_{r=1}^{k} c(k,r) = k!, \qquad \sum_{r=1}^{k} c(k,r)x^{r} = x(x+1)\cdots(x+k-1). \qquad (1.33)$$

The first identity reflects the fact that summing over all permutations with a fixed number of cycles r recovers the total number of permutations in S_k , while the second gives another combinatorial interpretation of c(k,r) as the coefficients in the power series of the 'rising factorial'.

1.2.2 The Action of Permutations on Quantum States

Throughout this course, we work with a *d*-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$, equipped with the standard orthonormal basis $\{|x\rangle\}_{x=0}^{d-1}$. Our main object of interest is the *k*-fold tensor product space $\mathcal{H}^{\otimes k} = (\mathbb{C}^d)^{\otimes k}$, often referred to as the *replica space* in the many-body literature.

Elements of the symmetric group S_k act naturally on this space by permuting the tensor factors. Concretely, given a permutation $\sigma \in S_k$, its action on a product basis state is defined as:

$$R_{\sigma}|x_{1}, x_{2}, \dots, x_{k}\rangle = |x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(k)}\rangle.$$
(1.34)

At first, the appearance of the inverse σ^{-1} might seem counterintuitive. To clarify this, consider an example with k = 4 and $\sigma = (1 \ 4 \ 3)(2) \in S_4$. Then $\sigma^{-1} = (1 \ 3 \ 4)(2)$, and we compute:

$$R_{\sigma}|x_1, x_2, x_3, x_4\rangle = |x_3, x_2, x_4, x_1\rangle.$$
(1.35)

This matches the effect of applying σ to the *tensor slots*: the content originally in position *j* is moved to position $\sigma(j)$. To write this as a reordering $\pi(i)$ of the vector indices *i*, we discover this permutation is exactly $\pi(i) = \sigma^{-1}(i)$ – thus justifying the use of the inverse in Eq. (1.34).

Equation (1.34) defines a linear (even unitary) operator R_{σ} on $\mathcal{H}^{\otimes k}$. The map

$$R: S_k \longrightarrow U(\mathcal{H}^{\otimes k}), \quad \sigma \mapsto R_{\sigma}$$
(1.36)

is a so-called *group representation* of S_k . This means it respects the group structure of S_k , more specifically:

$$R_{\pi\sigma} = R_{\pi}R_{\sigma}, \qquad R_{\sigma^{-1}} = R_{\sigma}^{-1}, \qquad R_{\sigma}^{\dagger} = R_{\sigma}^{-1}.$$
 (1.37)

These properties follow directly from the definition in Eq. (1.34). As an explicit verification of the composition law, let us define $\tilde{x}_i := x_{\sigma^{-1}(i)}$ and compute:

$$R_{\pi}R_{\sigma}|x_{1}, x_{2}, \dots, x_{k}\rangle = R_{\pi}|x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(k)}\rangle = |\tilde{x}_{\pi^{-1}(1)}, \dots, \tilde{x}_{\pi^{-1}(k)}\rangle$$
(1.38)

$$= |x_{(\sigma\pi)^{-1}(1)}, \dots, x_{(\sigma\pi)^{-1}(k)}\rangle = R_{\pi\sigma} |x_1, x_2, \dots, x_k\rangle.$$
(1.39)

This confirms that $R_{\pi\sigma} = R_{\pi}R_{\sigma}$, and also illustrates why the inverse in Eq. (1.34) is necessary: without it, the ordering of composition would be reversed, which is not consistent with the group structure.

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

Exercise 1.5. Verify that R defines a unitary representation of the symmetric group S_k , i.e., check Eq. (1.37).

Exercise 1.6. Show that permutations act on tensor products of operators as follows:

$$R_{\sigma}(A_1 \otimes A_2 \otimes \cdots \otimes A_k) R_{\sigma}^{\dagger} = A_{\sigma^{-1}(1)} \otimes A_{\sigma^{-1}(2)} \otimes \cdots \otimes A_{\sigma^{-1}(k)}.$$
(1.40)

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

$$((\mathbb{C}^q)^{\otimes n})^{\otimes k},\tag{1.41}$$

which can be naturally visualized as a $k \times n$ grid of qudits (see Fig. 1.1). 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

$$U^{\otimes k}$$
, where $U \in U((\mathbb{C}^q)^{\otimes n})$, (1.42)

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

$$((\mathbb{C}^q)^{\otimes n})^{\otimes k} \simeq ((\mathbb{C}^q)^{\otimes k})^{\otimes n},\tag{1.43}$$

then the permutation operator R_{π} acting on the full system decomposes as

$$R_{\pi} = r_{\pi}^{\otimes n},\tag{1.44}$$

where r_{π} acts on the *k*-dimensional replica space associated with each local qudit. This "horizontal" factorization is exactly what is depicted in Fig. 1.1 and will be essential in constructing efficient representations of randomized operations throughout the course.



Figure 1.1: 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 $U \in U(q^n)$ 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 $\gamma = (1, 2, ..., k)$. Then, we compute

$$\operatorname{tr}(R_{\gamma}) = \sum_{x_1,\dots,x_k=0}^{d-1} \langle x_1,\dots,x_k | R_{\gamma} | x_1,\dots,x_k \rangle$$
$$= \sum_{x_1,\dots,x_k} \langle x_1,\dots,x_k | x_k, x_1,\dots,x_{k-1} \rangle = \sum_{x_1,\dots,x_k} \delta_{x_1,x_k}\dots\delta_{x_k,x_{k-1}} = d. \quad (1.45)$$

Next, consider an arbitrary permutation σ . Then, we can find a permutation π such that $\pi\sigma\pi^{-1} = (1, \ldots, b_1)(b_1 + 1, b_1 + 2, \ldots, b_2) \cdots (b_{r-1} + 1, b_{r-1} + 2, \ldots, b_r)$ 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. 1.3). But $R_{\pi\sigma\pi^{-1}}$ is simply a tensor product of cyclic permutations on $\mathcal{H}^{\otimes b_1}, \ldots, \mathcal{H}^{\otimes (b_2 - b_1)}, \ldots, \mathcal{H}^{\otimes (b_r - b_{r-1})}$ and thus

$$\operatorname{tr}(R_{\sigma}) = \operatorname{tr}(R_{\pi\sigma\pi^{-1}}) = \prod_{i=1}^{r} d = d^{r} = d^{\#\sigma}.$$
 (1.46)

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 $tr(A_1 \otimes A_2 \otimes \cdots \otimes A_k R_{\sigma})$. Here, we can follow the same arguments as above: First, if $\sigma = \gamma = (1, ..., k)$ is the cyclic permutation, then

$$\operatorname{tr}(A_1 \otimes A_2 \otimes \cdots \otimes A_k R_{\gamma}) = \sum_{x_1, \dots, x_k} \langle x_1, \dots, x_k \, | \, A_1 \otimes A_2 \otimes \cdots \otimes A_k \, | \, x_k, x_1, \dots, x_{k-1} \rangle$$
(1.47)

$$=\sum_{x_1,\dots,x_k} (A_1)_{x_1,x_k} (A_2)_{x_2,x_1} \cdots (A_k)_{x_k,x_{k-1}} = \operatorname{tr}(A_k A_{k-1} \cdots A_1).$$
(1.48)

Next, for an arbitrary $\sigma = (a_1, \ldots, a_{j_1})(a_{j_1+1}, \ldots, a_{j_2}) \ldots (a_{j_{r-1}+1}, \ldots, a_k)$, find again a permutation π that 'orders the cycles' as $\pi \sigma \pi^{-1} = (1, \ldots, b_1)(b_1 + 1, b_1 + 2, \ldots, b_2) \cdots (b_{r-1} + 1, b_{r-1} + 2, \ldots, b_r)$ and then use Ex. **1.6** to conclude that

$$\operatorname{tr}(A_1 \otimes A_2 \otimes \cdots \otimes A_k R_{\sigma}) = \operatorname{tr}(A_{\pi^{-1}(1)} \otimes \cdots \otimes A_{\pi^{-1}(k)} R_{\pi\sigma\pi^{-1}})$$
(1.49)

$$= \operatorname{tr}(A_{\pi^{-1}(b_1)} \cdots A_{\pi^{-1}(1)}) \cdots \operatorname{tr}(A_{\pi^{-1}(b_r)} \cdots A_{\pi^{-1}(b_{r-1}+1)})$$
(1.50)

$$= \operatorname{tr}(A_{a_{j_1}} \cdots A_{a_1}) \cdots \operatorname{tr}(A_{a_k} \cdots A_{a_{r-1}+1}).$$
(1.51)

For the important case when $A_1 = A_2 = \cdots = A_k$, the final result is simplified to

$$\operatorname{tr}(A^{\otimes k}R_{\sigma}) = \prod_{c \in \lambda(\sigma)} \operatorname{tr}(A^{c}), \qquad (1.52)$$

where $\lambda(\sigma)$ is the cycle structure of the permutation σ .

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

$$\operatorname{Sym}_{k,d} \equiv \operatorname{Sym}((\mathbb{C}^d)^{\otimes k}) := \{ \psi \in (\mathbb{C}^d)^{\otimes k} \mid R_\sigma | \psi \rangle = | \psi \rangle \ \forall \sigma \in S_k \}.$$
(1.53)

We will now show that the projector onto $Sym_{k,d}$ is

$$P_{\operatorname{Sym},k,d} = \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} R_{\sigma}.$$
(1.54)

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

$$P_{\text{Sym},k,d}^{2} = \frac{1}{(k!)^{2}} \sum_{\sigma,\pi\in S_{k}} R_{\sigma\pi} = \frac{1}{k!} \sum_{\sigma\in S_{k}} \frac{1}{k!} \sum_{\tau\in S_{k}} R_{\tau} = P_{\text{Sym},k,d} , \qquad (1.55)$$

$$P_{\text{Sym},k,d}^{\dagger} = \frac{1}{k!} \sum_{\sigma \in S_k} R_{\sigma^{-1}} = \frac{1}{k!} \sum_{\pi \in S_k} R_{\pi} = P_{\text{Sym},k,d} , \qquad (1.56)$$

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 $\psi \in \text{Sym}_{k,d}$:

$$P_{\text{Sym},k,d}|\psi\rangle = \frac{1}{k!} \sum_{\sigma \in S_k} R_{\sigma} |\psi\rangle = \frac{1}{k!} \sum_{\sigma \in S_k} |\psi\rangle = |\psi\rangle, \qquad (1.57)$$

thus, 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

$$R_{\pi}|\psi\rangle = R_{\pi}P_{\text{Sym},k,d}|\psi\rangle = \frac{1}{k!}\sum_{\sigma\in S_{k}}R_{\pi\sigma}|\psi\rangle = \frac{1}{k!}\sum_{\tau\in S_{k}}R_{\tau}|\psi\rangle = P_{\text{Sym},k,d}|\psi\rangle = |\psi\rangle, \quad (1.58)$$

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. (1.46) and Ex. 1.4 as

$$\dim \operatorname{Sym}_{k,d} = \operatorname{tr} P_{\operatorname{Sym},k,d} = \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} d^{\#\sigma} = \frac{1}{k!} \sum_{r=1}^k c(k,r) d^r = \frac{d(d+1)\cdots(d+k-1)}{k!} = \binom{d+k-1}{k}.$$
(1.59)

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 permutation. Similar to the Feynman diagrammatics for perturbative expansions, this is simply a bookkeeping of the operation previously described.

We denote permutations as lines connecting the list $\{1, 2, ..., k\}$ to the output $\{\sigma(1), \sigma(2), ..., \sigma(k)\}$. For example, given $\tau = (12)(35)(4)$ a 5 elements permutation, we can represent it as

This notation is particularly useful, since it makes computing products particularly easy. For example, the product of τ with $\sigma = (123)(4)(5)$, we simply need to follow the lines after connecting them, specifically



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.

Traces require to add a curve that connect initial and final endpoints. For example:

$$\operatorname{tr}(R_{\sigma}) = \bigcup^{\#(\sigma)} = D^{\#(\sigma)}.$$
(1.62)

Similarly, for operators we have

$$\operatorname{tr}(A^{\otimes k}R_{\sigma}) = \begin{array}{c} & & \\ &$$

1.3 Further reading

QUANTUM RANDOMNESS I

2.1 What is a Haar measure?

On the real line \mathbb{R} , there is a unique measure *dx* with the following properties:

$$d(x+y) = dx$$
 (invariance), $\int_0^1 dx = 1$ (unit volume). (2.1)

It is the measure which we typically associate with a *uniform* distribution, as the invariance property guarantees that no point is preferred over another. Note that we cannot make this a probability measure on all of \mathbb{R} as it is non-compact and thus infinite measure. Here, we choose the interval [0, 1] for normalization and in this context *dx* is also called the *Lebesque measure*.

It turns out, that we can define a similar, invariant measure as long as the underlying set has a suitable group structure.¹ This invariant measure is called the *Haar measure*. Luckily, almost all groups we encounter are suitable; In particular, the unitary group U(d) is. The Haar measure dU on U(d) is then the unique measure such that

$$d(UV) = dU = d(VU)$$
 (left/right invariance), $\int_{U(d)} dU = 1$ (unit volume). (2.2)

In principle, integration over the Haar measure can be done using a suitable parametrization of unitaries. However, this is quite cumbersome and does not scale nicely with the dimension d. We will thus discuss smarter ways of integration in the next section.

[[M_H: *examples*, S¹, *discrete groups*]]

To capture typical behaviour of quantum dynamics, we will often draw unitaries 'uniformly at random'. Moreover, we will also see a few examples, where randomizing over unitaries can help in extracting information from a quantum system. In any case, uniform sampling refers to sampling from the probability measure *dU*. We also call such unitaries *Haar-random*.

Likewise, we can talk about *Haar-random states*. Although the set of states does not form a group, it is invariant under the unitary group in the sense that $U|\psi\rangle$ is another valid state. One can show that there is again a unique, unitarily invariant probability measure on the set of states, and a sample from this measure has the form $U|\psi\rangle$ for a fixed state $|\psi\rangle$ and a Haar-random *U*.

2.2 Haar integration and Weingarten calculus

In this section, we lay the foundations to compute integrals of the form

$$\mathsf{M}_{k}(A) := \int_{\mathsf{U}(d)} U^{\otimes k} A U^{\otimes k,\dagger} \mathsf{d} U \,. \tag{2.3}$$

As we will say in the later sections, these integrals are of fundamental importances for many applications in quantum information theory and many-body physics. To compute (2.3), we make use of the fact $M_k(A)$ lies in the subspace of operators that commute with $U^{\otimes k}$, the so-called *commutant*. A deep result in representation theory, the *Schur-Weyl duality*, states that a basis of this commutant is given by permutations, which will eventually allow us to compute M_k using *Weingarten calculus*.

¹To be mathematically precise, *G* should be a compact Hausdorff group.

2.2.1 The unitary commutant

In this section, we study the subspace of operators that commute with $U^{\otimes k}$, which we call the (*k*-fold) commutant of U(*d*):

$$\operatorname{Comm}_{k} = \left\{ A \in \operatorname{L}(\mathcal{H}^{\otimes k}) \mid U^{\otimes k}A = AU^{\otimes k} \,\forall U \in \operatorname{U}(d) \right\}.$$
(2.4)

We care about this because of the following, elementary observation:

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:

$$U^{\otimes k}BU^{\otimes k,\dagger} = \int_{\mathcal{U}(d)} (UV)^{\otimes k}A(UV)^{\otimes k,\dagger}dV = \int_{\mathcal{U}(d)} V^{\otimes k}AV^{\otimes k,\dagger}dV = B, \quad \forall U \in \mathcal{U}(d).$$
(2.5)

Thus, $B \in \text{Comm}_k$.

A central step in understanding the commutant is to note that the representation of S_k on $\mathcal{H}^{\otimes k}$ introduced in Sec. 1.2.2, this is $R_{\pi}|x_1, \ldots, x_k\rangle = |x_{\pi(1)}, \ldots, x_{\pi(k)}\rangle$, clearly commutes with $U^{\otimes k}$. In representation-theoretic terms, the representations of U(d) and S_k are said to be *dual to each other*. This implies that the permutations are contained in the unitary commutant, $R_{\pi} \in \text{Comm}_k$ for all $\pi \in S_k$. A fundamental result in representation theory, **Schur-Weyl duality**, even states that every element in the commutant is a linear combination of permutations. We will only state this result here and refer for a proof to the literature [tbd].

Theorem 2.1 (Schur-Weyl duality). *The k-fold unitary commutant* Comm_k *is spanned by* $\{R_\sigma | \sigma \in S_k\}$. *Vice versa, the commutant of* $\{R_\sigma | \sigma \in S_k\}$ *is spanned by* $\{U^{\otimes k} | U \in U(d)\}$

A natural question to ask is whether the 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 $d \ge k$.

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

$$R(\pi)|1,\ldots,k\rangle = |\pi(1),\ldots,\pi(k)\rangle.$$
(2.6)

Now, if $R(\pi)$ and $R(\sigma)$ would be linearly dependent ($\pi \neq \sigma$), than so would be the states $|\pi(1), \ldots, \pi(k)\rangle$ and $|\sigma(1), \ldots, \sigma(k)\rangle$. However, these are distinct elements from a basis, thus we arrive at a contradiction.

Remark 2.1. In fact, permutations become linearly dependent as soon as k > d. We do not need this statement in the following, thus we will not treat the proof in the lecture. We however state it here for completeness. We consider the antisymmetric subspace $\operatorname{Alt}_{k,d} \subset (\mathbb{C}^d)^{\otimes k}$ which is the joint -1 eigenspace of all transpositions R((ij)) for $(ij) \in S_k$. The projector onto $\operatorname{Alt}_{k,d}$ has the general form

$$P_{\text{Alt},k,d} = \frac{1}{k!} \sum_{\pi \in \mathbf{S}_k} \operatorname{sgn}(\pi) R(\pi) , \qquad (2.7)$$

where the sign function $sgn(\pi)$ is given as follows: Decompose π into transpositions only, then count the number of transpositions needed. If it is even, $sgn(\pi) = 1$, else $sgn(\pi) = -1$. Now, dim $Alt_{k,d} = {d \choose k} = 0$ if k > d, and hence $P_{Alt,k,d} = 0$. This gives a non-trivial linear relation between permutations, i.e. they are linearly dependent.

2.2.2 Weingarten calculus

By the previous findings, we can always write $M_k(A)$ as a linear combination

$$\mathsf{M}_k(A) = \sum_{\pi \in \mathsf{S}_k} c_\pi(A) R_\pi \,, \tag{2.8}$$

for some coefficients $c_{\pi}(A)$. Note that taking the trace inner product of $M_k(A)$ with a fixed permutation R_{σ}^{\dagger} yields

$$\operatorname{tr}(R^{\dagger}_{\sigma}\mathsf{M}_{k}(A)) = \int \operatorname{tr}(R^{\dagger}_{\sigma}U^{\otimes k}AU^{\otimes k,\dagger})dU = \int \operatorname{tr}(U^{\otimes k,\dagger}R^{\dagger}_{\sigma}U^{\otimes k}A)dU = \operatorname{tr}(R^{\dagger}_{\sigma}A).$$
(2.9)

However, we also have

$$\operatorname{tr}(R_{\sigma}^{\dagger}A) = \operatorname{tr}(R_{\sigma}^{\dagger}\mathsf{M}_{k}(A)) = \sum_{\pi \in \mathsf{S}_{k}} c_{\pi}(A) \operatorname{tr}(R_{\sigma}^{\dagger}R_{\pi}) =: \sum_{\pi \in \mathsf{S}_{k}} c_{\pi}(A) G_{\sigma,\pi}, \qquad (2.10)$$

where we defined the Gram matrix

$$G_{\pi,\sigma} := \operatorname{tr}(R_{\pi}^{\dagger}R_{\sigma}) = \operatorname{tr}(R_{\pi}^{\dagger}R_{\sigma}) = \operatorname{tr}(R_{\pi^{-1}\sigma}) = d^{\#(\pi^{-1}\sigma)}.$$
(2.11)

Here, we used that *R* is a representation to combine the product of permutation operators, and the trace formula (1.46). Setting $a_{\sigma} := \operatorname{tr}(R_{\sigma}^{\dagger}A)$, we can write the above equation in matrix form as a = Gc, which we could hope to invert to get an expression for the coefficient vector *c*. Note that the permutations are not orthogonal with respect to the trace inner product $(A|B) = \operatorname{tr}(A^{\dagger}B)$, and hence the Gram matrix is not simply diagonal. However, we know that the permutations span the commutant and that $M_k(A)$ lies in the commutant. Hence, the equation a = Gc always has a solution and it is unique if and only if the permutations form a basis, i.e. iff $d \ge k$, which is what will always assume for the remainder of this course.² Then, this solution is simply $c = G^{-1}a$, or put differently,

$$\mathsf{M}_{k}(A) = \sum_{\pi,\sigma\in\mathsf{S}_{k}} W_{\pi,\sigma} \operatorname{tr}(R_{\sigma}^{\dagger}A)R_{\pi}, \qquad (2.12)$$

where we defined $W := G^{-1}$, the so-called *Weingarten matrix*. Knowing the Weingarten matrix allows us to compute integrals of the form (2.3) using the Weingarten expansion (2.12).

Properties of the Gram and Weingarten matrix The Gram and Weingarten matrix have a substantial structure which directly relates to the representation theory of the symmetric group. We will not dive into these details in this course, but instead prove some concrete relations. We summarize them in the following.

Lemma 2.3. The Gram and Weingarten matrix fulfill the following properties.

- (a) $G_{\pi,\sigma}$ and $W_{\pi,\sigma}$ only depend on $\pi^{-1}\sigma$.
- (b) The row and column sums of G are constant:

$$\mathcal{G}_{k,d} := \sum_{\sigma} G_{\pi,\sigma} = \sum_{\pi} G_{\pi,\sigma} = \frac{(d+k-1)!}{(d-1)!} = d(d+1)\cdots(d+k-1).$$
(2.13)

(c) The row and column sums of W are constant:

$$\sum_{\sigma} W_{\pi,\sigma} = \sum_{\pi} W_{\pi,\sigma} = \mathcal{G}_{k,d}^{-1} = \frac{(d-1)!}{(d+k-1)!} \,. \tag{2.14}$$

²It is however not terribly complicated to make this work for d < k, see Sec. 2.4.

Proof. (a) Clearly, $G_{\pi,\sigma}$ depends only on $\pi^{-1}\sigma$ by definition (cf. Eq. (2.11)). Now note that this implies that *G* is invariant under simultaneous row and column permutations. Indeed, if T_{τ} is the permutation matrix acting as $T_{\tau}|e_{\pi}\rangle = |e_{\tau\pi}\rangle$, then $(T_{\tau}^{-1}GT_{\tau})_{\sigma,\pi} = G_{\tau\sigma,\tau\pi} = G_{\sigma,\tau}$. Inverting $G = T_{\tau}^{-1}GT_{\tau}$ yields $W = T_{\tau}^{-1}WT_{\tau}$ and thus $W_{\pi,\sigma} = W_{\tau\pi,\tau\sigma}$ for all τ , in particular $W_{\pi,\sigma} = W_{\mathrm{id},\pi^{-1}\sigma}$ for $\tau = \pi^{-1}$. For (b), we compute

$$\mathcal{G}_{k,d} = \sum_{\sigma} \operatorname{tr}(R_{\pi^{-1}\sigma}) = \sum_{\sigma} \operatorname{tr}(R_{\sigma}) = k! \operatorname{tr}(P_{\operatorname{Sym},k,d}) = k! \binom{d+k-1}{k} = \frac{(d+k-1)!}{(d-1)!}.$$
 (2.15)

Here, we used that the multiplication by π^{-1} can be absorbed into the sum (variable change), and the definition of the projector onto the symmetric subspace, $P_{\text{Sym},k,d} = \frac{1}{k!} \sum_{\sigma} R_{\sigma}$, and the value of its trace, cf. Eqs. (1.54) and (1.59). For (c), we note that the definition of *W* as inverse of *G* implies

$$\sum_{\pi} W_{\sigma,\pi} G_{\pi,\tau} = \delta_{\sigma,\tau} \qquad \Rightarrow \qquad 1 = \sum_{\pi,\tau} W_{\sigma,\pi} G_{\pi,\tau} = \mathcal{G}_{k,d} \sum_{\pi} W_{\sigma,\pi} \qquad \Rightarrow \qquad \sum_{\pi} W_{\sigma,\pi} = \mathcal{G}_{k,d}^{-1} .$$
(2.16)

Some examples and exercises In the following, we will compute the Weingarten matrix for small values of *k* and illustrate the computations of Haar integrals using a number of examples. To this end, we use that the Gram matrix has a very simple form: It is the trace of a permutation $R_{\tau} = R_{\pi}^{\dagger}R_{\sigma}$ and we gave an expression for this in Eq. (1.46).

Example 2.2.1: Weingarten matrix for k = 2

Let us consider k = 2. Then we only have two permutations: the identity $\mathbb{1}$ and the flip/swap $\mathbb{F} = (21)$. There is only one non-trivial matrix element, namely $G_{\mathbb{1},\mathbb{F}} = \text{tr}(\mathbb{F}) = d$. Hence, the Gram and Weingarten matrices are

$$G = d^2 \begin{pmatrix} 1 & d^{-1} \\ d^{-1} & 1 \end{pmatrix}, \qquad \qquad W = \frac{1}{d^2 - 1} \begin{pmatrix} 1 & -d^{-1} \\ -d^{-1} & 1 \end{pmatrix}.$$
(2.17)

Example 2.2.2: Average collision probability

The probability of obtaining the computational basis state *x* on $U|0\rangle$ is $p(x|U) = |\langle x | U | 0 \rangle|^2$. A measure of flatness of this distribution is the *collision probability*:

$$Z_U := \sum_{x} p(x|U)^2 = \sum_{x} |\langle x | U | 0 \rangle|^4.$$
(2.18)

Here, we are interested on how flat this distribution is *on average*, over Haar-random unitaries *U*. Due to the invariance of the Haar measure, we can simply absorb the *X* gates that prepare $|x\rangle = X^{x_1} \otimes \cdots \otimes X^{x_n} |0\rangle =: X(x) |0\rangle$ into the average:

$$Z := \int Z_U dU = \sum_x \int_U |\langle 0 | X(x)U | 0 \rangle|^4 dU = d \int_U |\langle 0 | U | 0 \rangle|^4 dU.$$
(2.19)

To compute the integral, we use second-order Weingarten calculus:

$$Z = d \int_{U} \operatorname{tr}(|0\rangle \langle 0|^{\otimes 2} U^{\otimes 2} |0\rangle \langle 0|^{\otimes 2} U^{\otimes 2,\dagger}) dU$$
(2.20)

$$= d \sum_{\pi,\sigma \in \mathbf{S}_2} W_{\pi,\sigma} \operatorname{tr}(R_{\sigma}^{\dagger}|0\rangle\langle 0|^{\otimes 2}) \operatorname{tr}(R_{\pi}|0\rangle\langle 0|^{\otimes 2})$$
(2.21)

$$=d\sum_{\pi,\sigma\in\mathbf{S}_2}W_{\pi,\sigma} \tag{2.22}$$

$$= 2d\mathcal{G}_{2,d}^{-1} = 2d\frac{(d-1)!}{(d+1)!} = \frac{2}{d+1}.$$
(2.23)

Here, we used Lem. 2.3. Note that we haven't actually used the exact form of the Weingarten matrix from Ex. 2.2.1. In fact, along the same lines we find that the average of $\sum_{x} p(x|U)^k$ is

$$I_k := \sum_{x} \int p(x|U)^k dU = k! d\mathcal{G}_{k,d}^{-1} = \frac{k! d!}{(d+k-1)!}.$$
 (2.24)

Exercise 2.1. Using Weingarten calculus, compute the operator $S := d \int (U|0) \langle 0|U^{\dagger} \rangle^{\otimes 2} dU$.

More properties – approximate orthogonality As stated before, permutations are not trace-orthogonal, however, their inner products become very small in large dimensions. This is sometimes called the *approximate orthogonality of permutations*. In general, the Gramian can be brought into the explicit form, by noting that the only permutation with exactly *k* disjoint cycles is the identity:

$$G_{\pi,\sigma} = d^k \left(\delta_{\pi,\sigma} + d^{-1} \underbrace{(1 - \delta_{\pi,\sigma}) d^{\#(\pi^{-1}\sigma) + 1 - t}}_{:= A_{\pi,\sigma}} \right),$$
(2.25)

Here, *A* is a matrix with zero diagonal and entries bounded by one. This allows us to formally invert *G*:

$$W = d^{-k} \left(\mathbb{1} + d^{-1}B \right), \qquad B := \sum_{j=0}^{\infty} (-1)^{j+1} d^{-j} A^{j+1}.$$
 (2.26)

This means, that both the Gram and Weingarten matrix are diagonally dominant, and that the offdiagonal entires are suppressed by 1/d. This reflects the fact that permutation become approximately orthogonal in large dimensions and thus

$$M_k(A) \approx d^{-k} \sum_{\pi} \operatorname{tr}(R_{\pi}^{\dagger} A) R_{\pi}$$
. (large dimensions) (2.27)

2.3 Approximating the Haar measure: Unitary designs

To be completed.

2.4 Further reading

MEASURING PROPERTIES OF MANY-BODY STATES

3.1 Shadow estimation: Expectation values through randomized measurements

To be completed.

3.2 Applications

QUANTUM RANDOMNESS II

4.1 Random quantum circuits

RANDOM DYNAMICS IN MANY-BODY SYSTEMS

5.1 Entanglement dynamics and membrane picture

To be completed.

5.2 Quantum scrambling in chaotic systems

APPENDIX A

SOME LINEAR ALGEBRA

This section gives a basic introduction to the linear algebraic concepts used in this course. Most of this should already be known from linear algebra and quantum mechanics lectures. At this point, the lectures notes are more detailed than the lecture to achieve a certain self-containement of the notes and provide a reference for later stages of the course.

A.1 States, operators, superoperators

State space As usual, quantum mechanics is modeled on a *Hilbert space* \mathcal{H} , which we take, in good quantum info tradition, to be *finite-dimensional* for the remainder of this course. Hence, we can simply think of $\mathcal{H} = \mathbb{C}^d$ with the standard basis $|x\rangle$ labeled by integers x = 0, 1, ..., d - 1, and the standard inner product

$$\langle \psi | \varphi \rangle = \sum_{x=0}^{d-1} \bar{\psi}_x \varphi_x , \qquad (A.1)$$

where $\psi_x = \langle x | \psi \rangle$ and $\varphi_x = \langle x | \varphi \rangle$ are the coefficients in the standard basis. Typically, we take vectors $\psi \in \mathcal{H}$ to be normalized: $\langle \psi | \psi \rangle = 1$.

The notation of the inner product as a 'bracket' motivates the popular *Dirac* or *bra-ket notation* which we adopt here: In this context, vectors $\psi \in \mathcal{H}$ are called *kets* and written as $|\psi\rangle$. The corresponding *bra* is a dual vector $\langle \psi | \in \mathcal{H}^*$ and given by the linear form $\mathcal{H} \ni \varphi \mapsto \langle \psi | \varphi \rangle$.¹ While the pairing between a bra and ket yields the inner product (the 'bracket'), the pairing between a ket and bra forms a so-called *outer product* $|\psi\rangle\langle\varphi|$ which is a linear operator on \mathcal{H} that acts as $\mathcal{H} \ni \chi \mapsto |\psi\rangle\langle\varphi|\chi\rangle$.

Linear operators The vector space of all linear operators $A : \mathcal{H} \to \mathcal{H}$ is denoted by $L(\mathcal{H})$. For any $A \in \mathcal{H}$, its *adjoint* A^{\dagger} is the linear operator for which

$$\langle \psi | A \varphi \rangle = \langle A^{\dagger} \psi | \varphi \rangle, \quad \forall \psi, \varphi \in \mathcal{H}.$$
 (A.2)

If represented in an orthonormal basis, such as the standard basis, the adjoint operator is the conjugate transpose matrix, $A^{\dagger} = \overline{A}^{\top}$.

Definition A.1. *In the following, we define some relevant classes of operators:*

- Hermitian (or self-adjoint) operator: $A \in L(\mathcal{H})$ such that $A^{\dagger} = A$. Hermitian operators have only real eigenvalues and an orthonormal eigenbasis.
- Unitary operator: $U \in L(\mathcal{H})$ such that $U^{\dagger}U = UU^{\dagger} = \mathbb{1}$.
- Positive semi-definite (psd) operator: Hermitian A ∈ L(H) with only non-negative eigenvalues. We write A ≥ 0.
- Projector: Hermitian $P \in L(\mathcal{H})$ such that $P^2 = P$.
- Quantum state: $\rho \in L(\mathcal{H})$ such that $\rho \ge and \operatorname{tr} \rho = 1$. ρ is called pure if it is a projector: $\rho^2 = \rho$. Pure states have rank one and are of the form $\rho = |\psi\rangle\langle\psi|$.

Finally, the unitaries on \mathcal{H} *form the* unitary group U(\mathcal{H}) = U(d).

¹In mathematics, this is called the *Riesz representation theorem*.

The vector space $\text{End}(\mathcal{H})$ of linear operators on \mathcal{H} forms a Hilbert space of dimension (dim \mathcal{H}) = d^2 in its own right with the *Hilbert-Schmidt* or *trace inner product*:

$$(X|Y) \coloneqq \operatorname{tr}(X^{\dagger}Y). \tag{A.3}$$

In particular, we can introduce an orthonormal operator basis as a set of operators A_1, \ldots, A_{d^2} such that $(A_i | A_j) = \delta_{ij}$. We will now introduce an import example of such a basis, the *Pauli basis*.

Example A.1.1: Pauli basis

Recall the Pauli operators

$$\sigma_{0,1} \equiv X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_{1,1} \equiv Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_{1,0} \equiv Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (A.4)$$

which we complement with the identity $\sigma_{0,0} = \mathbb{1}$. Then, the multi-qubit Pauli operators on $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ are simply given by all possible tensor products of the single-qubit Pauli operators, in formula:

$$\sigma_a := \sigma_{a_1, a_2} \otimes \cdots \otimes \sigma_{a_{2n-1}, a_{2n}}, \quad a \in \mathbb{Z}_2^{2n}.$$
(A.5)

Pauli operators are orthogonal, $(\sigma_a | \sigma_b) = 2^n \delta_{a,b}$. In particular, the normalized Pauli operators $\hat{\sigma}_a = 2^{-n/2} \sigma_a$ form an orthonormal operator basis. Note that Pauli operators can be generalized to arbitrary dimensions and they give rise to an orthonormal operator basis in any of those.

We leave it as an exercise to show some basic properties of Pauli operators.

Exercise A.1 (Properties of Pauli operators). Using the definition of Pauli operators, Eq. (A.5), show the following properties:

- (a) $\sigma_a^{\dagger} = \sigma_a$ and $\sigma_a^2 = 1$, *i.e.* the multi-qubit Pauli operators are both Hermitian and unitary.
- (b) $\sigma_a \sigma_b \propto \sigma_{a+b}$, where addition is in \mathbb{Z}_2^{2n} , i.e. modulo two.
- (c) $\sigma_a \sigma_b = (-1)^{[a,b]} \sigma_b \sigma_a$ where $[a,b] := \sum_{i=1}^n a_i b_{n+i} + a_{n+i} b_i$.
- (d) $(\sigma_a | \sigma_b) = 2^n \delta_{a,b}$.

Superoperators and quantum channels Following a common nomenclature, we refer to linear maps ϕ : $L(\mathcal{H}) \rightarrow L(\mathcal{H})$ as *superoperators* (on \mathcal{H}). We call ϕ *positivity-preserving* or simply *positive* iff $\phi(A) \ge 0$ for all $A \ge 0$. As it turns out, positive maps are not necessarily positive when we let them act on a subsystem of a composite system, i.e. if we consider $\phi \otimes id_{\mathcal{A}}$ for some auxillary system \mathcal{A} . Thus, we say that ϕ is *completely positive* iff $\phi \otimes id_{\mathcal{A}}$ is positive for any auxillary system \mathcal{A} . Completely positive maps are the ones which we consider 'physical', as the map quantum states to quantum states. This leads us to the definition of a quantum channel:

Definition A.2 (Quantum channel). A quantum channel is a superoperator ϕ that is completely positive and trace-preserving, this is $\phi \otimes id_{\mathcal{A}}$ is positive for any auxiliary system \mathcal{A} and $tr(\phi(A)) = tr(A)$ for all $A \in L(\mathcal{H})$. We call ϕ unital iff $\phi(\mathbb{1}) = \mathbb{1}$.

Example A.1.2: Quantum channels

Some examples of quantum channels are the following:

- Unitary channels: $\phi(X) = UXU^{\dagger}$ for $U \in U(\mathcal{H})$.
- *Mixed-unitary channels*: $\phi(X) = \sum_i \lambda_i U_i X U_i^{\dagger}$ for $U_i \in U(\mathcal{H})$, $\lambda_i \ge 0$, and $\sum_i \lambda_i = 1$. These are convex combinations of unitary channels.
- Dephasing channel: $\phi(X) = \sum_{x} \langle x | X | x \rangle \langle x |$.
- *Reset channels*: $\phi(X) = tr(X)\rho$ for a fixed quantum state ρ .

To denote superoperators, it is handy to introduce an 'operator Dirac notation' as follows: In analogy to the usual Dirac notation, we use the Hilbert-Schmidt inner product to define *operator kets and bras* by $|Y) \equiv Y$ and $(X| : Y \mapsto (X|Y)$. Likewise, we can define outer products |X)(Y| which are now linear maps on $L(\mathcal{H})$, i.e. superoperators, acting as $A \mapsto (Y|A)X$.

The 'operator bra-ket notation' is especially useful to expand a superoperator in an operator basis, i.e. write down its matrix representation. Typically, we will use the (normalized) Pauli basis in this context, but any orthonormal basis works similarly. To this end, we observe that $id = \sum_{a} |\hat{\sigma}_{a}\rangle(\hat{\sigma}_{a}|$ and thus

$$\phi = \sum_{a,b} |\hat{\sigma}_a| (\hat{\sigma}_a |\phi| \hat{\sigma}_b) (\hat{\sigma}_b| =: \sum_{a,b} \phi_{a,b} |\hat{\sigma}_a) (\hat{\sigma}_b|$$
(A.6)

The matrix $(\phi_{a,b})_{a,b}$ is the representation of ϕ in the Pauli basis. For quantum channels, this matrix has certain properties, which we here leave as an exercise:

Exercise A.2. Let ϕ be a multi-qubit quantum channel and let $(\phi_{a,b})_{a,b}$ be its matrix representation in the *Pauli basis. Show that*

- (a) $(\phi_{a,b})_{a,b}$ is real.
- (b) $\phi_{a,0} = \delta_{a,0}$. If ϕ is unital, it also holds $\phi_{0,b} = \delta_{0,b}$, hence $\phi \simeq \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$.
- (c) Suppose ϕ is a Pauli channel, this is $\phi(X) = \sum_a \lambda_a \sigma_a X \sigma_a^{\dagger}$ (for convex coefficients λ_a). Then, $(\phi_{a,b})_{a,b}$ is diagonal (use Ex. A.1).

Norms Throughout this paper, we use *Schatten p-norms* which are defined for any linear map $X \in L(\mathcal{V}, \mathcal{W})$ between Hilbert spaces \mathcal{V} and \mathcal{W} and $p \in [1, \infty]$ as

$$\|X\|_p := \left(\operatorname{tr}|X|^p\right)^{\frac{1}{p}} = \left(\sum_{i=1}^d \sigma_i^p\right)^{\frac{1}{p}},\tag{A.7}$$

where $|X| \coloneqq \sqrt{X^{\dagger}X} \in L(\mathcal{V})$ and $\sigma_i \ge 0$ are the singular values of *X*, i.e. the square roots of the eigenvalues of the positive semidefinite operator $X^{\dagger}X$. In particular, we use the *trace norm* p = 1, the *Hilbert-Schmidt norm* p = 2, and the *spectral norm* $p = \infty$. The definition of Schatten norms only relies on the Hilbert space structure of the underlying vector space, thus these norms can be defined for operators and superoperators alike.

A.2 Non-orthonormal bases

Let $(f_i)_{i \in [d]}$ be a basis of a Hilbert space \mathcal{V} . Thus, every $v \in \mathcal{V}$ has a unique expansion $v = \sum_i v_i f_i$. If $(f_i)_i$ is orthonormal, then the coefficients v_i can be simply expressed as $v_i = \langle f_i | v \rangle$. This can be generalized to arbitrary bases by introducing the concept of a *dual basis* $(\tilde{f}_i)_i$ which is defined by the linear system of equations

$$\langle \tilde{f}_i | f_j \rangle = \delta_{i,j} \,. \tag{A.8}$$

As $(f_i)_i$ is a basis, this system has a unique solution. It is now straightforward to verify that

$$\langle \tilde{f}_i | v \rangle = \sum_j v_j \langle \tilde{f}_i | f_j \rangle = v_i.$$
(A.9)

Moreover, this implies that

$$\left(\sum_{i} |f_i\rangle \langle \tilde{f}_i|\right)(v) = \sum_{i} v_i f_i = v, \qquad (A.10)$$

for all $v \in \mathcal{V}$ and hence $\sum_i |f_i\rangle \langle \tilde{f}_i| = \mathrm{id}_{\mathcal{V}}$.

The dual basis can be computed using the Gram matrix

$$G_{i,j} := \langle v_i | v_j \rangle. \tag{A.11}$$

One can show that *G* is generally positive semi-definite and since the v_i are linearly independent, the eigenvalues are in fact strictly larger than zero. Hence, it is invertible and we define its inverse as $W := G^{-1}$. Then, the dual basis can be expressed as

$$\tilde{v}_i := \sum_j W_{i,j} v_j \,. \tag{A.12}$$

Indeed:

$$\langle \tilde{v}_i | v_j \rangle = \sum_k W_{i,k} \langle v_k | v_j \rangle = \sum_k W_{i,k} G_{k,j} = \delta_{i,j} \,. \tag{A.13}$$