Basics of Group Representation Theory

The Unitary Group and Random Quantum States

Markus Döring
University of Heidelberg

November 12, 2013

1 Preface

This is the written report corresponding to my talk in the seminar *Selected topics in Mathematical Physics: Quantum information theory*. The seminar was lead by Prof. Dr. Manfred Salmhofer, executive director of the Institute for Theoretical Physics at the University of Heidelberg, and Dr. Markus Müller, junior research group leader at that institute.

2 Motivation

In fields like statistical dynamics or chaos theory, we use probabilistic models to come to conclusions about the state and the evolution of a system. If we want to apply quantum theory to these fields, it would be helpful to know whether a state whose classical analog is chaotic is effectively random [Woo90].

For the definition of a *random quantum state* we need at least a probability measure on the set of quantum states. It turns out that the *Haar measure* can be seen as a probability measure, and that some results of group representation theory allow us to calculate some results for random quantum states.

In this seminar talk, we will start with some basics on the unitary group, followed by a bit of group representation theory. We will then introduce the Haar measure as a probability measure on the unitary group, and we will close with the calculation of expectation values of random pure states:

$$\mathbb{E}(|\psi\rangle) = \int |\psi\rangle \ \mathrm{d}|\psi\rangle. \tag{2.1}$$

3 The Unitary Group

In this section, we are going to review some basic results for unitary matrices and the so called unitary group $U(n)$. We will omit the proofs, because they are actually neither hard nor new.

Definition 3.1. (operator norm)
The operator norm of a matrix $A \in \mathbb{C}^{n\times n}$ is defined as

$$\|A\|_{\text{op}} \coloneqq \max_{\substack{|\varphi\rangle\in\mathbb{C}^n \\ \langle\varphi|\varphi\rangle=1}} \|A\,|\varphi\rangle\,\|_2 = \max_{\substack{|\varphi\rangle\in\mathbb{C}^n \\ \langle\varphi|\varphi\rangle=1}} \langle\varphi|A^\dagger A|\varphi\rangle\,. \tag{3.2}$$

Definition 3.2. (the unitary group)
A matrix $U \in \mathbb{C}^{n\times n}$ is called unitary, if $U^\dagger U = \mathbb{1}_n$. The set

$$U(n) \coloneqq \left\{U \in \mathbb{C}^{n\times n} :\ U \text{ is unitary}\right\} \tag{3.3}$$

is called the unitary group[1].

Proposition 3.3. *(some properties of unitary matrices)*
Let $U \in U(n)$ and $|\varphi\rangle \in \mathbb{C}^n$.

(a) $U \in U(n) \Leftrightarrow U^\dagger \in U(n)$

(b) $U, V \in U(n) \Rightarrow UV \in U(n)$

(c) $\|U\,|\varphi\rangle\,\|_2 = \|\,|\varphi\rangle\,\|_2$

(d) $U = \sum_{i=1}^{n} u_i\,|\varphi_i\rangle\,\langle\varphi_i|$ *for some orthonormal base* $\{|\varphi_i\rangle\,,\ 1 \le i \le n\}$ *of* $\mathbb{C}^n$ *and eigenvalues* $u_i \in \mathbb{C},\ |u_i| = 1$ *(U is unitarily diagonalizable)*

(e) $\operatorname{tr}(UAU^\dagger) = \operatorname{tr}(A)$ *for all* $A \in \mathbb{C}^{n\times n}$

(f) $\|AU\|_{\text{op}} = \|UA\|_{\text{op}} = \|A\|_{\text{op}}$ *for all* $A \in \mathbb{C}^{n\times n}$

Definition 3.4. (complete, totally bounded)
Let (M, d) be a metric space.

- (M, d) is totally bounded if it can be covered by a finite set of ε-balls for all $\varepsilon > 0$, i.e.

$$\forall\varepsilon > 0\ \exists n \in \mathbb{N}, x_1, \ldots, x_n \in M \text{ such that } M \subseteq \bigcup_{i=1}^{n}\{x \in M :\ d(x, x_i) < \varepsilon\} \tag{3.4}$$

[1] The term *group* will be clarified in the next section.

- (M, d) is complete if every Cauchy sequence converges in M, i.e.

$$\begin{aligned} &\{x_k\}_{k\in\mathbb{N}} \subset M \text{ with } \forall \varepsilon > 0\ \exists N \in \mathbb{N} \text{ such that } \forall k, l > N:\ d(x_k, x_l) < \varepsilon \\ \Rightarrow &\lim_{k\to\infty} x_k \in M \end{aligned} \tag{3.5}$$

Theorem 3.5. *(Heine-Borel for general metric spaces, see every analysis textbook)*
A metric space (M, d) is compact if and only if it is complete and totally bounded.

Proposition 3.6.
The unitary group $U(n)$ is compact.

Proof. Let $\{U_k\}_{k\in\mathbb{N}}$ be a Cauchy sequence in the metric space $(U(n), \|\cdot\|_{\text{op}}$[2]. We know that $\mathbb{C}^{n\times n}$ is complete, so there is a limit $U \in \mathbb{C}^{n\times n}$ with $\lim_{k\to\infty} U_k = U$. Define the sequence $D_k \coloneqq U_k - U$.

$$\begin{aligned} \left\|U^\dagger U - \mathbb{1}_n\right\|_{\text{op}} &= \lim_{k\to\infty} \left\|(U_k + D_k)^\dagger (U_k + D_k) - \mathbb{1}_n\right\|_{\text{op}} \\ &= \lim_{k\to\infty} \left\|U_k^\dagger D_k + D_k^\dagger U_k + D_k^\dagger D_k\right\|_{\text{op}} \\ &\leq \lim_{k\to\infty} 2\left\|D_k\right\|_{\text{op}} + \left\|D_k\right\|_{\text{op}}^2 = 0 \end{aligned} \tag{3.6}$$

Therefore, $U \in U(n)$ and $U(n)$ is complete.

We can embed the unitary group $U(n)$ into the euclidean space $\mathbb{R}^{2n^2}$ by the map

$$f : (u_{ij})_{1\leq i,j\leq n} \mapsto (\mathfrak{Re}(u_{11}), \mathfrak{Im}(u_{11}), \mathfrak{Re}(u_{12}), \mathfrak{Im}(u_{12}), \ldots)^{\mathrm{T}}. \tag{3.7}$$

Since every entry u_{ij} of a unitary matrix is bounded by $|u_{ij}| \leq 1$, we see that the image of $U(n)$ in $\mathbb{R}^{2n^2}$ is bounded, and thus $U(n)$ is bounded as well.

With theorem 3.5, $U(n)$ is compact. □

There is another intuitive analogue: We can associate the vectors in $\mathbb{C}^n$ with vectors in $\mathbb{R}^{2n}$ like in equation 3.7 and observe the effect of unitary matrices on vectors on the $2n-1$-sphere $S^{2n-1} \coloneqq \{x \in \mathbb{R}^{2n} :\ \|x\|_2 = 1\}$. As it turns out the effect is just rotation and reflection at the origin: the unitaries act like parts of the symmetry group of the unit sphere, $\mathrm{O}(2n, \mathbb{R})$. This will be of help when we want to explain the properties of a measure on pure states later on.

[2]The choice of a matrix norm does not matter too much, but the operator norm has the nice property of being invariant to unitary transformations.

4 Unitary Group Representations

As the next step we will introduce the notion of *group representation* and examine its implications for the statistical properties that we want to analyze. For a more detailed view on the subject, refer to [BTD10][3]. Most of the upcoming definitions are analog to the ones given there, but simplified to our use case where possible.

Let us start with some basic notation conventions and definitions.

Notation 4.1.
We will use the following naming conventions throughout the next section. Let V be a complex vector space of dimension $0 < n < \infty$. Denote the set of maps from V to itself as $\mathrm{End}(V)$ (endomorphisms on V) and the invertible endomorphisms on V as $\mathrm{Aut}(V)$ (automorphisms on V).

Definition 4.2. (groups and group homomorphisms)
A *group* $(G, \cdot)$ is a set G combined with a multiplication operator that fulfills the following axioms:

Closure $\forall g, h \in G : \; g \cdot h \in G$

Associativity $\forall g, h, i \in G : \; (g \cdot h) \cdot i = g \cdot (h \cdot i)$

Existence of Identity $\exists e \in G \; \forall g \in G : \; g \cdot e = e \cdot g = g$

Existence of Inverse $\forall g \in G \; \exists g^{-1} \in G : \; g \cdot g^{-1} = e$

A group homomorphism is a map between two groups $(G, \cdot), (H, \circ)$ that preserves the group structure, i.e.

$$\begin{aligned} f : \quad & G \to H \\ & g \mapsto f(g) \end{aligned} \tag{4.8}$$

$$\forall u, v \in G : \quad f(u \cdot v) = f(u) \circ f(v) \tag{4.9}$$

$$f(u^{-1}) = f(u)^{-1} \tag{4.10}$$

Example 4.3. The unitary group $U(n)$ is a group with identity element $\mathbb{1}$ and inverse elements $U^{-1} = U^\dagger$.

Definition 4.4. (group representation, G-module)
A group homomorphism

$$\begin{aligned} U_{(\cdot)} : \quad & G \to \mathrm{Aut}(V) \\ & g \mapsto U_g \end{aligned} \tag{4.11}$$

[3] or any other textbook on group representations

is called a *group representation* of G on V, and V is then referred to as a G-module. If $U_g \in U(n)\ \forall g \in G$, we call U a *unitary group representation*. If $U_{(\cdot)}$ is bijective, the representation is called *faithful*.

Example 4.5. (standard representation)
Consider the group $(U(n), \cdot)$. The representation $U \mapsto U$ is obviously a unitary representation of the unitary group. We call it the *standard representation*.

We want to restrict ourselves to unitary representations in this section, but most results also apply to general representations as well, because every group representation can be seen as a unitary representation with respect to some specific inner product (see [BTD10], p. 68f, for details).

Definition 4.6. (G-submodule, irreducibility)
Let U_g be a unitary group representation of group G on V. A subspace $V_1 \subseteq V$ is called invariant (under the group action), if

$$\forall g \in G, |v\rangle \in V_1 :\ U_g |v\rangle \in V_1. \tag{4.12}$$

An invariant subspace V_1 of V is also called a *G-submodule* of V.

If the only G-submodules of V are V and $\{0\}$, we call V an irreducible G-module and U_g an *irreducible representation*. Otherwise, we call both *reducible*. G-submodules that are not trivial (i.e. $\{0\}$ or V) are called *proper G-submodules*.

Example 4.7.
Consider the unitary representation

$$\begin{aligned} U_{(\cdot)} : U(n) &\to \mathrm{Aut}(\mathbb{C}^n \otimes \mathbb{C}^n) \\ U &\mapsto U \otimes U. \end{aligned} \tag{4.13}$$

It is a reducible representation with the invariant subspaces

$$\mathbb{C}^n_{\mathrm{sym}} \coloneqq \{|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n :\ \mathbb{F}(|\psi\rangle) = |\psi\rangle\} \tag{4.14}$$

$$\mathbb{C}^n_{\mathrm{antisym}} \coloneqq \{|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n : \mathbb{F}(|\psi\rangle) = -|\psi\rangle\}, \tag{4.15}$$

where $\mathbb{F}$ denotes the flip operator:

$$\mathbb{F}(|\varphi\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |\varphi\rangle. \tag{4.16}$$

Proof. We can choose the bases of the respective subspaces as

$$B^n_{\text{sym}} = \left\{ \frac{1}{\sqrt{2}}(|\varphi_i\varphi_j\rangle + |\varphi_j\varphi_i\rangle) : \ 1 \leq i \leq n, i < j \leq n \right\} \cup \{|\varphi_i\varphi_i\rangle : \ 1 \leq i \leq n\} \quad (4.17)$$

$$B^n_{\text{antisym}} = \left\{ \frac{1}{\sqrt{2}}(|\varphi_i\varphi_j\rangle - |\varphi_j\varphi_i\rangle) : \ 1 \leq i \leq n, i < j \leq n \right\}. \quad (4.18)$$

for some orthonormal base $\{|\varphi_i\rangle : \ 1 \leq i \leq n\}$ of $\mathbb{C}^n$. From

$$(U \otimes U)(|\varphi_i\varphi_j\rangle + a\,|\varphi_j\varphi_i\rangle) = U\,|\varphi_i\rangle \otimes U\,|\varphi_j\rangle + aU\,|\varphi_j\rangle \otimes U\,|\varphi_i\rangle = |\tilde{\varphi}_i\tilde{\varphi}_j\rangle + a\,|\tilde{\varphi}_j\tilde{\varphi}_i\rangle \quad (4.19)$$

we see that the subspaces are in fact invariant with respect to the group action $U \otimes U$. □

Proposition 4.8.
Let U_g be a unitary group representation of the group G on the G-module V.

(a) If $V_1 \subset V$ is a G-submodule, then there is a G-submodule $V_2 \perp V_1$ with $V = V_1 \oplus V_2$.

(b) The G-module V is the direct sum of irreducible, pairwise orthogonal G-submodules.

(c) The decomposition of V into orthogonal irreducible G-submodules is unique.

Proof. Let V_1 be a G-submodule of V. If $V_1 = V$ or $V_1 = \{0\}$, the proposition (a) is trivial. Let therefore $m \in \{1, \ldots, n-1\}$ be the dimension of V_1. We can choose an orthonormal base $|u_i\rangle, 1 \leq i \leq m$ of V_1 and extend it to an orthonormal base $|u_i\rangle, 1 \leq i \leq n$ of V. Now we observe the group action on these base vectors. For an arbitrary, but fixed $g \in G$, we write U_g with respect to this base as

$$U_g = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\,|u_i\rangle\,\langle u_j|\,. \quad (4.20)$$

The group action on $|u_k\rangle, 1 \leq i \leq m$ is therefore

$$U_g\,|u_k\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\,|u_i\rangle\,\langle u_j|u_k\rangle = \sum_{i=1}^{n} a_{ik}\,|u_i\rangle\,. \quad (4.21)$$

This vector must lie in $\text{span}(\{|u_k\rangle, 1 \leq k \leq m\})$, and thus $\forall 1 \leq k \leq m, m < i \leq n : a_{ik} = 0$. We can apply the same argument to the representation $U_{g^{-1}} = U_g^\dagger$, and find that for all $1 \leq k \leq m,\ m < i \leq n :\ a_{ki} = 0$. We can now write

$$U_g = \left(\sum_{i=1}^{m}\sum_{j=1}^{m} a_{ij}\,|u_i\rangle\,\langle u_j|\right) + \left(\sum_{i=m+1}^{n}\sum_{j=m+1}^{n} a_{ij}\,|u_i\rangle\,\langle u_j|\right), \quad (4.22)$$

which shows us that V_2 is also invariant under the group action, and therefore V_2 is a G-submodule of V.

The second part of the proposition is easily shown by induction over the dimension n: apply the arguments given here on the G-submodules V_1 and V_2 recursively, and recall that they have both dimension strictly less than n.

The uniqueness is also a simple conclusion. Assume there are two distinct sets of irreducible G-submodules $V_1, \ldots, V_k$ and $W_1, \ldots, W_m$. Then (without loss of generality, just reordered) $V_1 \cap W_1 \supsetneq \{0\}$, $V_1 \neq W_1$ and $W_1 \supsetneq V_1 \cap W_1$. Let $|v\rangle \in V_1 \cap W_1 \setminus \{0\}$, then by definition 4.6 $U_g |v\rangle \in V_1$ and $U_g |v\rangle \in W_1$ and thus $U_g |v\rangle \in V_1 \cap W_1$. This means that $V_1 \cap W_1$ is a proper G-submodule of W_1, which is a contradiction. □

This proposition also provides us with some insight about the structure of reducible group representations. As we can see in equation 4.22, all the representation matrices are in fact block diagonal matrices with respect to the chosen orthonormal base, and therefore to any orthonormal base constructed from bases of the irreducible submodules.

The following result, Schur's Lemma, is a key ingredient for calculating statistical properties of random states, like the expectation value. In most of the literature available, Schur's lemma is stated in terms of morphisms between G-modules, but we will use a less general version in terms of matrices, because it is sufficient for the calculation of the properties that we are interested in.

Lemma 4.9. *(Issai Schur 1905)*
Let U_g be a unitary representation of the group G on the complex vector space V. If a diagonalizable matrix A commutes with U_g for all $g \in G$, then A can be written as a linear combination of the projectors onto the invariant subspaces of V, i.e.

$$A = \sum_{i=1}^{m} \lambda_i \pi_i, \tag{4.23}$$

with $\lambda_i \in \mathbb{C}$ and

$$\pi_i \coloneqq \sum_{j \in I_i} |u_j\rangle \langle u_j| \tag{4.24}$$

for an orthonormal base $\{|u_j\rangle : \ j \in I_i \subseteq \{1, \ldots, n\}\}$ of V_i as in proposition 4.8.

Proof. We can state the commutativity of A as

$$AU_g = U_g A \quad \forall g \in G. \tag{4.25}$$

Let $|v\rangle \in \mathbb{C}^n \setminus \{0\}$ be an eigenvector of A and $\lambda \in \mathbb{C}$ be an eigenvalue to this eigenvector, i.e. $A |v\rangle = \lambda |v\rangle$. Then

$$AU_g |v\rangle = U_g A |v\rangle = \lambda U_g |v\rangle , \tag{4.26}$$

and thus $U_g |v\rangle$ is as well an eigenvector to the eigenvalue λ. This holds for all U_g, and therefore the eigenspace $S_\lambda = \{|v\rangle \in v : A |v\rangle = \lambda |v\rangle\}$ is an invariant subspace under the

unitary representation U_g. By proposition 4.8, the partition of V into irreducible subspaces is unique, so $S_\lambda = \bigoplus_{i \in I_\lambda} V_i$, with G-submodules V_i of V and some (non-empty) index set I_λ. The matrix A is diagonalizable, so $\bigoplus_{\lambda \in \sigma(A)} S_\lambda = V$. As previously shown in proposition 4.8, we can choose the orthonormal base $\{|u_i\rangle : \ 1 \leq i \leq n\}$ of V such that it contains orthonormal bases for all irreducible G-submodules V_i. Those base vectors are all eigenvectors of A, and therefore V has an orthonormal base of eigenvectors of A, and thus A is unitarily diagonalizable:

$$A = \sum_{i=1}^{n} \tilde{\lambda}_i \, |u_i\rangle \langle u_i| = \sum_{j=1}^{m} \lambda_j \pi_j. \tag{4.27}$$

Note that λ_i (and obviously $\tilde{\lambda}_i$) are not neccessarily distinct. □

Example 4.10. Let us go back to example 4.7. For an orthonormal base $\{|\varphi_i\rangle : \ 1 \leq i \leq n\}$ of $\mathbb{C}^n$ we know that $\{|\varphi_i \varphi_j\rangle : \ 1 \leq i \leq n \, 1 \leq j \leq n\}$ is a base of $\mathbb{C}^n \otimes \mathbb{C}^n$. For these base vectors, we get

$$\begin{aligned} \mathbb{F}\left(U \otimes U \, |\varphi_i \varphi_j\rangle\right) &= \mathbb{F}\left(U \, |\varphi_i\rangle \otimes U \, |\varphi_j\rangle\right) = \left(U \, |\varphi_j\rangle\right) \otimes \left(U \, |\varphi_i\rangle\right) \\ &= (U \otimes U)\mathbb{F}(|\varphi_i \varphi_j\rangle) \end{aligned} \tag{4.28}$$

for an arbitrary $U \in U(n)$. Therefore, $(U \otimes U)\mathbb{F}$ is the same action as $\mathbb{F}(U \otimes U)$ on all base vectors of $\mathbb{C}^n \otimes \mathbb{C}^n$, and thus the operators commute. We can apply Schur's lemma 4.9 and get

$$\mathbb{F} = \pi_{\text{sym}} - \pi_{\text{antisym}} \tag{4.29}$$

for the appropriate projectors on the subspaces $\mathbb{C}^n_{\text{sym}}, \mathbb{C}^n_{\text{antisym}}$.

Corollary 4.11. *(Schur's Lemma for irreducible unitary representations)*
Let $U_\cdot$ be an irreducible unitary representation of the group G on the complex vector space V. If a matrix A commutes with U_g for all $g \in G$, then A is a scalar matrix, i.e.

$$A = \lambda \mathbb{1}_n, \ \lambda \in \mathbb{C}. \tag{4.30}$$

Proof. The matrix A has at least one eigenvector $|v\rangle \in V \setminus \{0\}$ with eigenvalue $\lambda \in \mathbb{C}$. We use the same argument as in lemma 4.9, and conclude that the eigenspace S_λ is an invariant subspace of V with respect to U_g. We know that $v \in S_\lambda$, and so by definition 4.6, it must be $S_\lambda = V$. That means that λ is the only eigenvalue of A, and thus $A = \lambda \mathbb{1}_n$. □

5 The Haar Integral

In this section we are going to establish a probability measure on the unitary group. As seen in section 3, there is a relation of the unitary group of dimension n to the unit sphere in $\mathbb{R}^{2n}$. A probability measure on this sphere could be considered fair, or evenly distributed, if

a change of orientation of a set does not change its probability. This would be the case if we take the probability proportional to the spheric area of the set. As it turns out, the Haar measure is equivalent to this notion of a probability distribution on the sphere (see [Chr70]).

Due to the lack of time we will not go through all of the proofs in this section. The curious reader is encouraged to refer to some textbooks on measure theory for the general results. Results specific to the Haar measure can be found in [Nac76], but also in many other books available.

Notation 5.1. We will sometimes abuse notation and use the terms measure and integral exchangeable. This is not a problem though, because we can always construct an integral from a given measure, and we get the measure from the integral by setting

$$\mu(A) \coloneqq \int_G \chi_A(x)\ \mathrm{d}\mu(x) \tag{5.31}$$

for a Borel set $A \subseteq G$ and the *characteristic function* χ.

We also want to introduce a short-hand notation for the translation of sets:

$$gA = \{gh \in G :\ h \in A\}, \quad g \in G,\ A \subseteq G \text{ Borel set} \tag{5.32}$$

$$Ag = \{hg \in G :\ h \in A\}, \quad g \in G,\ A \subseteq G \text{ Borel set.} \tag{5.33}$$

Definition 5.2. (positive integral)
An integral μ is said to be *positive*, if it is positive for all continuous, μ-integrable functions f with compact support.

Lemma 5.3. *(e.g. in [Nac76], p. 21)*
If μ is a positive integral on a locally compact space G, then the integral μ is a continuous map from $\mathcal{C}(K)$ to $\mathbb{R}$ for all compact subsets of G with respect to the uniform norm

$$\|f\|_{\sup} \coloneqq \left|\sup_{x\in K}(f(x))\right|. \tag{5.34}$$

Definition 5.4. (left- and right-invariant integrals)
An integral μ on the group G is *left-invariant*, if

$$\int_G f(gx)\ \mathrm{d}\mu(x) = \int_G f(x)\ \mathrm{d}\mu(x) \tag{5.35}$$

or *right-invariant*, if

$$\int_G f(xg)\ \mathrm{d}\mu(x) = \int_G f(x)\ \mathrm{d}\mu(x) \tag{5.36}$$

for all $g \in G$ and all μ-integrable functions f.

Example 5.5. (Lebesgue measure)

Consider the group $(\mathbb{R}^n, +)$. The Haar measure for this group is the Lebesgue measure:

$$\int_{\mathbb{R}^n} f(x+y)\ \mathrm{d}\lambda(x) = \int_{\mathbb{R}^n} f(y+x)\ \mathrm{d}\lambda(x) = \int_{\mathbb{R}^n} f(x)\ \mathrm{d}\lambda(x), \quad \forall y \in \mathbb{R}^n. \tag{5.37}$$

Theorem 5.6. *(Alfréd Haar, John von Neumann 1933; see [Nac76], p. 65ff.)*
On every locally compact group G exists at least one left-invariant positive integral. If μ, ν are both left-invariant positive integrals on G, then there is a constant factor $c > 0$ such that $\nu = c\mu$.

Corollary 5.7. *Let G be a compact group.*

(a) The Haar-measure on G is finite.

(b) Every left-invariant Haar measure on G is also a right-invariant Haar-Measure on G.

(c) There is a unique left- and right-invariant measure μ on G with $\mu(G) = 1$.

Proof. We will prove the finiteness indirectly. Assume that $\mu(G) = \infty$. We construct the sequence

$$f_n(x) \coloneqq \frac{1}{n}, \quad n \in \mathbb{N}, \tag{5.38}$$

which clearly converges to 0 with respect to the uniform norm. With lemma 5.3 we get

$$0 = \int_G \lim_{n\to\infty} f_n(x)\ \mathrm{d}\mu(x) = \lim_{n\to\infty} \int_G f_n(x)\ \mathrm{d}\mu(x) = \lim_{n\to\infty} \frac{1}{n}\infty = \infty, \tag{5.39}$$

which is a contradiction. Thus $\mu(G) < \infty$ holds.

Let μ be a left-invariant measure on G and define the measure $\nu(A) \coloneqq \mu(Ag)$ for Borel sets A and some fixed $g \in G$. Then ν is obviously also a left-invariant measure on G and by uniqueness

$$\exists c > 0 : \quad \nu = c\mu. \tag{5.40}$$

We proved already that $\mu(G) < \infty$, what gives us

$$c\mu(G) = \nu(G) = \mu(Gg) = \mu(G) \Leftrightarrow c = 1 \Leftrightarrow \mu = \nu. \tag{5.41}$$

We conclude that μ is also right-invariant:

$$\mu(Ag) = \nu(A) = \mu(A). \tag{5.42}$$

The last statement is a simple consequence of the other two. □

The (normalized) Haar measure on the unitary group can thus be seen as a probability measure, and we will use it to *draw unitaries at random* in the next section.

6 Conclusion and Outlook

We will conclude this report with an application of Schur's Lemma on random quantum states, as promised.

Example 6.1. (expectation value of random pure states)[4]
We can model a *random pure quantum state* $\rho = |\psi\rangle\langle\psi|$ as some initial state $\rho_0 = |\psi_0\rangle\langle\psi_0|$ that is transformed by a (Haar-)random unitary matrix U. We get

$$\mathbb{E}(\rho) = \int |\psi\rangle\langle\psi| \ \mathrm{d}\,|\psi\rangle = \int_{U(n)} U\,|\psi_0\rangle\langle\psi_0|\,U^\dagger \ \mathrm{d}\mu(U). \tag{6.43}$$

Note that this integral does not depend on the initial state ρ_0 because of the left-invariance of the Haar integral.

We see that $\mathbb{E}(\rho)$ is self-adjoint and thus (unitarily) diagonalizable. Furthermore, for any unitary matrix Q, we get

$$\begin{aligned} Q\,\mathbb{E}(\rho) &= \int_{U(n)} QU\rho U^\dagger \ \mathrm{d}\mu(U) \\ &= \int_{U(n)} W(U)\rho W(U)^\dagger Q \ \mathrm{d}\mu(U) \\ &= \int_{U(n)} W\rho W^\dagger Q \ \mathrm{d}\mu(W) = \mathbb{E}(\rho)Q \end{aligned} \tag{6.44}$$

by substitution $W(U) = QU$ and the left-invariance of the Haar integral. Therefore, all prerequisites for lemma 4.9 are met, and we can write

$$\mathbb{E}(\rho) = \lambda\mathbb{1}_n \tag{6.45}$$

for some $\lambda \in \mathbb{C}$. The trace operator is linear, so we can exchange the integral and the trace operator and get

$$n\lambda = \mathrm{tr}(\mathbb{E}(\rho)) = \int_{U(n)} U\,\mathrm{tr}(|\psi_0\rangle\langle\psi_0|)U^\dagger \ \mathrm{d}\mu(U) = \int_{U(n)} \mathrm{d}\mu(U) = 1 \tag{6.46}$$

and this gives us the final result for the expectation value of a random pure state,

$$\mathbb{E}(\rho) = \frac{1}{n}\mathbb{1}_n, \tag{6.47}$$

the maximally mixed state.

Over the course of the next talks, the results given here will be refined and applied to bipartite Hilbert spaces (a small system interacting with the universe). One proposition will

[4] As you may have noticed, we did not formally define an integral as a map from functions to matrices. We assume at this point that we can use the standard definition of matrix functions, acting on the eigenvalues.

be that *almost all pure states are almost maximally entangled*, which has some interesting implications on statistical mechanics [PSW06].

References

[BTD10] Bröcker, Theodor ; Tom Dieck, Tammo: *Representations of compact lie groups*. New York [u.a.] : Springer, 2010 (Graduate texts in mathematics ; 98 ; Graduate texts in mathematics 98). – ISBN 978–3–642–05725–0

[Chr70] Christensen, Jens Peter R.: On Some Measures Analogous to Haar Measure. In: *Mathematica Scandinavica* 26 (1970), S. 103–106

[Nac76] Nachbin, Leopoldo: *The Haar integral*. Repr. Huntington, NY : Krieger, 1976. – ISBN 0–88275–374–6 ; 978–0–88275–374–4

[PSW06] Popescu, Sandu ; Short, Anthony J. ; Winter, Andreas: Entanglement and the foundations of statistical mechanics. In: *Nature Physics* 2 (2006), Nr. 11, S. 754–758

[Woo90] Wootters, William K.: Random quantum states. In: *Foundations of Physics* 20 (1990), Nr. 11, 1365–1378. http://dx.doi.org/10.1007/BF01883491. – DOI 10.1007/BF01883491. – ISSN 0015–9018