Representations & Quantum Information

Notes for MATH 595RQT, Aniket Deshpande
As instructed by Felix Leditzky

"The universe is an enormous direct product of representations of symmetry groups." – Steven Weinberg

Contents

Preface

these notes are a work in progress. they will be updated throughout the semester.

1 A Review of Quantum Information

1.1 Quantum States & Systems

A *quantum system* is a physical system with quantum-mechanical degres of freedom:

- positions and momenta of particles
- polarizations of photons
- spins of particles

Note that these degrees of freedoms can be discrete or continuous. We will discuss the spin of an electron. There are two *basis states*, spin up and spin down. Each of these is assigned a vector in $\mathbb{C}^2$, the state space.

$$|\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |\downarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

By the *superposition principle*, a quantum state can be prepared in a state $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. The state $|\psi\rangle$ is a *pure state*. The probabilities of finding an electron in spin-up or spin-down states are given by

$$\mathbf{Pr}(\uparrow) = |\langle\uparrow|\psi\rangle|^2 = |\alpha|^2, \quad \mathbf{Pr}(\downarrow) = |\langle\downarrow|\psi\rangle|^2 = |\beta|^2.$$

Formally, the state space of a quantum system is given by a *Hilbert space* $\mathcal{H}$, a complete complex inner-product space. We will be restricting our attention to finite-dimensional Hilbert spaces $\mathcal{H} \cong \mathbb{C}^d$.

Definition 1 (Observables). Observable quantities are represented by *Hermitian* operators

$$A \in \{X \in \mathcal{L}(\mathcal{H}) \mid X^\dagger = X\}.$$

The real eigenvalues of A can be experimentally measured.

A state of a quantum system assigns an expectation value of observable; it describes the expected measurement statistics of an observable in a quantum system. States are identified by *density operators* $\rho \in \mathcal{L}(\mathcal{H})$ [1].

Definition 2 (Density Operators). A density operator $\rho \in \mathcal{L}(\mathcal{H})$ satisifies

- $\rho \geq 0$, i.e., $\langle\phi|\rho\psi\rangle \geq 0$ for all $\phi \in \mathcal{H}$. *(positivity)*
- $\mathbf{Tr}\,\rho = 1$. *(normalization)*

The expectation of an observable A with respect to a state ρ is given by

$$\mathbf{E}[A] = \mathbf{Tr}\left(A\rho\right).$$

The set of density operators of a finite-dimensional Hilbert space $\mathcal{H}$ is denoted by $\mathcal{D}(\mathcal{H})$. This set is compact and convex. That is, if $\rho_i \in \mathcal{D}(\mathcal{H})$ and λ_i are probabilities, then $\rho = \sum_i \lambda_i \rho_i \in \mathcal{D}(\mathcal{H})$.

[1] Here, $\mathcal{L}(\mathcal{H})$ denotes the space of linear operators on $\mathcal{H}$.

Definition 3 (Pure & Mixed States). A *pure state* is a density operator $\rho \in \mathcal{D}(\mathcal{H})$ of the form

$$\rho = |\psi\rangle\langle\psi|$$

for some normalized vector $|\psi\rangle \in \mathcal{H}$. *Mixed states* must be written as a convex combination of pure states:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

This collection of state vectors $\{|\psi_i\rangle\}$ with probabilities $\{p_i\}_i$ is a *pure state ensemble* for the mixed state ρ.

Every mixed quantum state has infinitely many pure-state ensembles to realize it. Every quantum state also has a *spectral decomposition* with its eigenvalues and eigenvectors:

$$\rho = \sum_i \lambda_i |v_i\rangle\langle v_i|$$

where λ_i are the eigenvalues and $\{|v_i\rangle\}$ are an orthonormal basis of eigenvectors of ρ. By the definition of density operators, we have that $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. Hence, the eigenvalues of a density matrix form a probability distribution.

1.2 Measurements

Definition 4 (Projective Measurements). Let A be an observable on a quantum system $\mathcal{H}$ with respect to state ρ. Consider the spectral decomposition of A:

$$A = \sum_\alpha x_\alpha P_\alpha$$

where x_α are the eigenvalues of A and P_α are orthogonal projectors on their corresponding eigenspaces. These projectors satisfy

- $P_\alpha \geq 0$, in particular, $P_\alpha^\dagger = P_\alpha$. *(positive semi-definiteness)*
- $P_\alpha P_\beta = \delta_{\alpha,\beta} P_\alpha$ for all α, β. *(orthogonality)*
- $\sum_\alpha P_\alpha = \mathbb{1}$. *(completeness)*

$\{P_\alpha\}_\alpha$ is called a *projective measurement* of A that gives the values x_α with probabilities $p_\alpha = \mathbf{Tr}\left(P_\alpha \rho\right)$.

Definition 5 (POVMs). A collection of operators $\{E_k\}_k$ with $E_k \geq 0$ and $\sum_k E_k = \mathbb{1}$ is called a *positive operator-valued measure* (POVM). For each effect operator E_k, the outcome k is measured with probability $p_k = \mathbf{Tr}\left(E_k \rho\right)$.

POVMs are more general than projective measurements, as they do not require the effects to be orthogonal.

1.3 Entanglement & Composite Systems

Consider quantum systems A and B with respective Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The joint system AB is described by the *tensor product* of the two Hilbert spaces $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. A density operator ρ_{AB} lies in $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$, which is isomorphic to $\mathcal{L}(\mathcal{H}_A) \otimes \mathcal{L}(\mathcal{H}_B)$.

A *marginal* state ρ_A of a bipartite state ρ_{AB} is defined with the *partial trace*

$$\mathrm{Tr}\left(\rho_A X_A\right) = \mathrm{Tr}\left(\rho_{AB}(X_A \otimes \mathbb{1}_B)\right)$$

for all $X_A \in \mathcal{L}(\mathcal{H}_A)$. The marginal state ρ_A is the state of system A when system B is ignored. Similarly, we can define the marginal state ρ_B of system B. This uniquely defines the partial trace as a linear map $\mathrm{Tr}_B : \mathcal{L}(\mathcal{H}_{AB}) \to \mathcal{L}(\mathcal{H}_A)$. If $\{|e_i\rangle_B\}_i$ is an orthonormal basis for $\mathcal{H}_B$, then

$$\mathrm{Tr}_B X_{AB} = \sum_{i=1}^{\dim B} (\mathbb{1}_A \otimes \langle e_i|_B) X_{AB} (\mathbb{1}_A \otimes |e_i\rangle_B).$$

There can be various types of correlation between systems A and B. We distinguish them here.

(i) *Product States*: $\rho_{AB} = \omega_A \otimes \sigma_B$ for states ω_A and σ_B. For a product state, any local measurements (done with partial traces) do not affect the other system. A and B are completely uncorrelated.

(ii) *Separable States*: $\rho_{AB} = \sum_i p_i \omega_A^{(i)} \otimes \sigma_B^{(i)}$ for states $\omega_A^{(i)}$ and $\sigma_B^{(i)}$ and a probability distribution $\{p_i\}_i$. Conditioned on i, the state $\omega_A^{(i)} \otimes \sigma_B^{(i)}$ is uncorrelated.

(iii) *Entangled States*: ρ_{AB} cannot be written as a convex combination of product states. These states describe quantum correlations that cannot be explained classically.

For example, consider $\mathbb{C}^2$ and its computational basis $\{|0\rangle, |1\rangle\}$. The state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}.$$

The corresponding density operator is

$$\rho_{\Phi^+} = |\Phi^+\rangle\langle\Phi^+| = \frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}.$$

This is the *Bell state*,[2] is *not* separable. In fact, it is NP-hard to determine whether a given mixed state is separable. However, for pure states there exists an efficient criterion based on the singular-value decomposition.

[2] Also called the EPR state or the maximally-entangled state.

Remark 1. In fact, we can define four more such maximally-entangled states on $\mathbb{C}^2 \otimes \mathbb{C}^2$ of the form

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B), \quad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B). \tag{1}$$

The four states $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$ form an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$, known as the *Bell basis*. We call them *maximally entangled* becaue for each state, both marginals on A and B are maximally mixed.

$$\mathbf{Tr}_A\, \Phi^+_{AB} = \mathbf{Tr}_B\, \Phi^+_{AB} = \frac{1}{2}\mathbb{1}_A = \frac{1}{2}\mathbb{1}_B, \tag{2}$$

and similarly for the other three states.

To show that Φ^+ is entangled, the obvious approach is to show that there is no way to write the state as a convex combination of product states. However, there is a much more elegant (and useful) method of proving that Φ^+ is not separable via the *PPT criterion*. Let us quickly define the *partial transpose* $(\cdot)^{T_B} := \mathbf{id}_A \otimes (\cdot)^T_B$. In a coordinate basis, we define operator bases $\{Q_{A,i}\}_i$ for $\mathcal{L}(\mathcal{H}_A)$ and $\{P_{B,j}\}_j$ for $\mathcal{L}(\mathcal{H}_B)$. Then the partial transpose of a bipartite operator $X_{AB} = \sum_{i,j} x_{i,j} Q_{A,i} \otimes P_{B,j}$ is given by

$$X_{AB}^{T_B} = \sum_{i,j} x_{i,j} Q_{A,i} \otimes P_{B,j}^{T_B}.$$

A state ρ_{AB} is *positive under partial transpose* (PPT) if $\rho_{AB}^{T_B} \geq 0$. The partial transpose develops the following separability criterion.

Proposition 1 (PPT Criterion). Every separable state ρ_{AB} is PPT.[3]

Proof. Let $\rho_{AB} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}$ be a separable state. Then this means that $\rho^{(i)}, \rho_B^{(i)} \geq 0$, and $p_i \geq 0$. Since the partial transpose is a linear map and a state $X \in \mathcal{L}(\mathcal{H}) \geq 0$ if and only if $X^T \geq 0$, we have

$$\rho_{AB}^{T_B} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)T_B} \geq 0,$$

as a convex combination of positive semidefinite operators. □

We can use this criterion to show that Φ^+ is entangled. First, let us compute its partial transpose.

$$2\left(\Phi^+\right)^{T_B} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}_B^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =: \mathbb{F}_{AB}.$$

The operator $\mathbb{F}_{AB}$ is the *swap operator*. It acts on $\mathbb{C}^2 \otimes \mathbb{C}^2$ by swapping the two systems.

$$\mathbb{F}_{AB}\left(|\phi\rangle + |\psi\rangle\right) = |\psi\rangle \otimes |\phi\rangle, \quad \textit{for all } |\phi\rangle, |\psi\rangle \in \mathbb{C}^2. \tag{3}$$

[3] Hence, if $\rho_{AB}^{T_B}$ has a negative eigenvalue, then ρ_{AB} is entangled.

It follows that the Bell states are *eigenvectors* of the swap operator, with eigenvalues of ± 1. Thus, Φ^+ is entangled since it is an eigenvector of $\mathbb{F}_{AB}$ with a negative eigenvalue. Unfortunately, the PPT criterion is only a necessary condition for separability, not a sufficient one. It was proven that it *is* sufficient for small dimensions $d \leq 6$, but quantum states that are both PPT and entangled exist for larger dimensions.[4] Such states are called *bound entangled* states. In general, it is NP-hard to determine whether a given mixed state is separable. However, we can use a singular value decomposition to develop and efficiently checkable separability criterion for bipartite mixed states.

Definition 6 (Schmidt Decomposition). Let $|\psi\rangle_{AB}$ be a pure bipartite quantum state. Then there exists sets of orthonormal vectors $\{|e_i\rangle\}_{i=1}^r$ and $\{|f_j\rangle\}_{j=1}^s$ such that

$$|\psi\rangle_{AB} = \sum_{i=1}^{r} \sqrt{\lambda}_i |e_i\rangle_A \otimes |f_i\rangle_B$$

with strictly positive real λ_i. These are *Schmidt coefficients* and satisfy $\sum_{i=1}^r \lambda_i = 1$. The integer r is the *Schmidt rank* of $|\psi\rangle_{AB}$.

Proposition 2. $|\psi\rangle_{AB}$ is entangled if and only if $r > 1$.

Proof. If $r = 1$, then the Schmidt decomposition gives $|\psi\rangle_{AB} = \sqrt{\lambda_1}|e_1\rangle_A \otimes |f_1\rangle_B$, which is a product state and hence separable. Suppose for contradiction that $|\psi\rangle_{AB}$ is separable, so $|\psi\rangle_{AB} = |a\rangle_A \otimes |b\rangle_B$ for some states $|a\rangle_A$ and $|b\rangle_B$. This is already in Schmidt form with only one term, giving Schmidt rank $r = 1$. This contradicts our assumption that $r > 1$. Therefore, $|\psi\rangle_{AB}$ must be entangled. □

The marginals of $|\psi\rangle_{AB}$ are given by partial traces

$$\rho_A = \mathrm{Tr}_B \psi_{AB} = \sum_{i=1}^{r} \lambda_i |e_i\rangle\langle e_i|_A, \quad \rho_B = \mathrm{Tr}_A \psi_{AB} = \sum_{i=1}^{r} \mu_j |f_i\rangle\langle f_i|_B.$$

These are spectral decompositions; ρ_A and ρ_B have the same spectrum given by the Schmidt coefficients and the *Schmidt vectors* $\{|e_i\rangle_A\}$ and $\{|f_i\rangle_B\}$ are the eigenvectors of ρ_A and ρ_B, respectively. The entanglement of a bipartite state can be quantified by the *entanglement entropy*, which we will discuss later.

Definition 7 (Purification). Let $\rho_A \in \mathcal{D}(\mathcal{H})$ be a mixed quantum state. Any state $|\psi\rangle_{AR} \in \mathcal{H}_A \otimes \mathcal{H}_R$ satisfying $\mathrm{Tr}_R \psi_{AR} = \rho_A$ where $\mathcal{H}_R$ is some auxiliary Hilbert space, is a *purification* of ρ_A.

Proposition 3. For a mixed state ρ_A, a purification exists on $\mathcal{H}_A \otimes \mathcal{H}_R$ with $\dim \mathcal{H}_R \geq \operatorname{rank} \rho_A$.

Proof. Consider the spectral decomposition $\rho_A = \sum_{i=1}^n \lambda_i |v_i\rangle\langle v_i|_A$, where $\lambda_i > 0$ such that $r = \operatorname{rank} \rho_A$. Take $\mathcal{H}_R = \mathbb{C}^r$ with orthonormal basis $\{|w_i\rangle_R\}_{i=1}^r$, then $|\psi\rangle_{AR} := \sum_{i=1}^r \sqrt{\lambda_i} |v_i\rangle_A \otimes |w_i\rangle_R$ is a purification of ρ_A. □

[4] See [HHH96] for the proof.

Proposition 4. Let $|\psi\rangle_{AR_1}$ and $|\varphi\rangle_{AR_2}$ be two purifications of ρ_A. Without loss of generality, assume $\dim R_1 \leq \dim R_2$. Then there exists an isometry $V : \mathcal{H}_{R_1} \to \mathcal{H}_{R_2}$ such that

$$|\varphi\rangle_{AR_2} = (\mathbb{1}_A \otimes V)|\psi\rangle_{AR_1}.$$

Proof. This follows from the Schmidt decomposition. □

1.4 Distance Measures

We require ways to analyze how close two quantum states are. Approximating states are commonly quantified using these measures. We will focus on fidelity and the trace norm.

Definition 8 (Trace Norm). For a linear operator $X \in \mathcal{L}(\mathcal{H})$, the *trace norm* is defined as

$$\|X\|_1 = \operatorname{Tr}\sqrt{X^\dagger X} = \sum_{i=1}^{d} S_i(X),$$

where $d = \dim \mathcal{H}$ and $S_i(X)$ are the singular values of X.

This defines a norm (in the standard analytical sense) on $\mathcal{L}(\mathcal{H})$. In the case when X is Hermitian with real eigenvalues λ_i, we have $\|X\|_1 = \sum_i |\lambda_i|$.

Definition 9 (Trace Distance). Let ρ and σ be quantum states on $\mathcal{H}$. Their *trace distance* is defined as

$$D(\rho,\sigma) := \frac{1}{2}\left\|\rho - \sigma\right\|_1.$$

We discuss some properties of the trace distance.

(i) $D(\cdot,\cdot)$ is non-negative, symmetric, and satisfies the triangle inequality, making it a metric.

(ii) $D(\cdot,\cdot)$ is bounded to the interval $[0,1]$ and $D(\rho,\sigma) = 0$ if and only if $\rho = \sigma$. With $\operatorname{supp} X := (\ker X)^\perp$, we also have $D(\rho,\sigma) = 1$ if and only if $\operatorname{supp}\rho \perp \operatorname{supp}\sigma$.

(iii) $D(\rho,\sigma) = D(U\rho U^\dagger, U\sigma U^\dagger)$ for all unitaries U and $D(\rho_A,\sigma_A) \leq D(\rho_{AB},\sigma_{AB})$.

(iv) $D(\rho,\sigma) = \sup\left\{\operatorname{Tr}\left[P(\rho-\sigma)\right] \mid P \geq 0 \text{ and } \mathbb{1} - P \geq 0\right\}$.

(v) $D(\rho,\sigma)$ is related to the maximum probability of distinguishing ρ and σ.

Definition 10 (Fidelity). The *fidelity* $F(\rho,\sigma)$ of quantum states ρ and σ is defined as

$$F(\rho,\sigma) := \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1 = \operatorname{Tr}\left(\sigma^{1/2}\rho\sigma^{1/2}\right)^{1/2}.$$

We discuss some useful properties of fidelity.

(i) $F(\cdot,\cdot)$ is bounded to $[0,1]$ and $F(\rho,\sigma) = 1$ if and only if $\rho = \sigma$. $F(\rho,\sigma) = 0$ if and only if $\operatorname{supp}\rho \perp \operatorname{supp}\sigma$.

(ii) $F(\rho,\sigma) = F(\sigma,\rho)$, but F is not a metric.

(iii) $F(\rho,\sigma) = F(U\rho U^\dagger, U\sigma U^\dagger)$ for all unitaries U and $F(\rho_A,\sigma_A) \geq F(\rho_{AB},\sigma_{AB})$.

(iv) F is jointly concave:

$$F\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \geq \sum_i p_i F(\rho_i, \sigma_i).$$

(v) For pure states $|\psi\rangle$ and $|\varphi\rangle$, $F(\psi,\varphi) = \big|\langle\psi|\varphi\rangle\big|$.

Theorem 1 (Uhlmann's Theorem). Let ρ and σ be quantum states on $\mathcal{H}$. Then

$$F(\rho,\sigma) = \sup\left\{\big|\langle\psi|\varphi\rangle\big| \,:\, |\psi\rangle \text{ is a purification of } \rho \text{ and } |\varphi\rangle \text{ is a purification of } \sigma\right\}.$$

Proof. Let the states act on $\mathcal{H}_A$. Fix an auxiliary space $\mathcal{H}_R$ with $\dim \mathcal{H}_R \geq \dim \mathcal{H}_A$ and define the "canonical" purifications via spectral decompositions

$$\rho = \sum_i \lambda_i |i\rangle\langle i| \;\Rightarrow\; |\psi_\rho\rangle := \sum_i \sqrt{\lambda_i}\,|i\rangle_A |i\rangle_R, \qquad \sigma = \sum_j \mu_j |j\rangle\langle j| \;\Rightarrow\; |\phi_\sigma\rangle := \sum_j \sqrt{\mu_j}\,|j\rangle_A |j\rangle_R.$$

By the uniqueness of purifications up to isometry on R, every purification of ρ is of the form $(\mathbb{1}_A \otimes U_R)|\psi_\rho\rangle$ for some unitary U_R on $\mathcal{H}_R$. Hence

$$\langle\psi\big|\varphi\rangle = \langle\psi_\rho\big|(\mathbb{1}_A \otimes U_R)\big|\phi_\sigma\rangle = \sum_{i,j} \sqrt{\lambda_i \mu_j}\, \underbrace{\langle i|j\rangle}_{\langle i|j\rangle} \underbrace{R\langle i|\,U_R\,|j\rangle R}_{\langle i|U_R|j\rangle} = \mathrm{Tr}(U_R X),$$

where the operator on $\mathcal{H}_R \cong \mathcal{H}_A$ is

$$X := \sum_{i,j} \sqrt{\lambda_i \mu_j}\,\langle i|j\rangle\, |i\rangle\_R\langle j| = \sqrt{\rho}\,\sqrt{\sigma}.$$

The last equality is basis-free: it is exactly the matrix product $\sqrt{\rho}\,\sqrt{\sigma}$ expressed in the eigenbases $\{|i\rangle\}$ and $\{|j\rangle\}$.

We now maximize the absolute inner product over all unitaries U_R and use the variational characterization of the trace norm.

Lemma. For any operator X, $\sup\big|\mathrm{Tr}(UX)\big| = \|X\|_1$, where U is any unitary.

Sketch. Let $X = W|X|$ be the polar decomposition. Then $\mathrm{Tr}(W^\dagger X) = \mathrm{Tr}\,|X| = \|X\|_1$ and Hölder's inequality gives $|\mathrm{Tr}(UX)| \leq \|X\|_1$ for all U. □

Applying the lemma with $X = \sqrt{\rho}\,\sqrt{\sigma}$ yields

$$\sup_{\text{purifications } |\psi\rangle, |\varphi\rangle} \big|\langle\psi|\varphi\rangle\big| = \sup_{U_R} \big|\mathrm{Tr}(U_R\,\sqrt{\rho}\,\sqrt{\sigma})\big| = \big\|\sqrt{\rho}\,\sqrt{\sigma}\big\|_1 = F(\rho,\sigma),$$

which is exactly the desired identity, with the maximizing unitary given by the partial isometry from the polar decomposition of $\sqrt{\rho}\,\sqrt{\sigma}$. This also shows the supremum is attained. □

Proposition 5 (The Fuchs-van de Graaf Inequalities). For any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$,

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

The proof of this can be found in [FvdG99].

2 A Review of Representation Theory

Representation theory is the study of groups through group actions on vector spaces. We begin with establishing some basic definitions.

2.1 Actions & Representations

Definition 11 (Group). A *group* $(G,\cdot)$ is a set G equipped with a binary operation $\cdot : G \times G \to G$ satisfying

- *Associativity*: $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ for all $a,b,c \in G$.
- *Identity*: There exists an element $e \in G$ such that $e\cdot g = g\cdot e = g$ for all $g \in G$.
- *Inversibility*: For each $g \in G$, there exists an element $g^{-1} \in G$ such that $g\cdot g^{-1} = g^{-1}\cdot g = e$.

Example 1. Given a field $(\mathbb{F},\cdot,+)$, then $(\mathbb{F},+)$ is a group [5].

Example 2. The collection of bijections from $\{1,2,\dots,n\}$ to itself is the *symmetric group* S_n.

Example 3. The set of invertible linear maps with entries on vector space V is the *general linear group* $\mathrm{GL}(V)$.

We now define what it means for a group to *act* on a vector space.

Definition 12 (Group Action). An *action* on a group G on a set X is a map $\varphi : G \times X \to X$ such that

$$\varphi(g,\varphi(h,x)) = \varphi(gh,x) \quad \text{and} \quad \varphi(e,x) = x$$

for all $g,h \in G$ and $x \in X$.

Definition 13 (Representation). A *representation* (φ,V) of a group G on a vector space V (over field $\mathbb{F}$) is a group homomorphism $\varphi : G \to \mathrm{GL}(V)$.

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{for all } g_1,g_2 \in G$$

A representation will always satisfy $\varphi(e) = \mathbb{1}_V$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$. The *dimension* or *degree* of a representation (φ,V) is the dimension of the vector space V. In this course, we will deal with finite-dimensional representations.

Example 4. Let G be a cyclic group of order d, generated by g. Let $V = \mathbb{C}^d$ with basis $|0\rangle, |1\rangle, \dots, |d-1\rangle$. Consider a linear operator X on V defined by $X|i\rangle = |i+1 \bmod d\rangle$ for all i. Then the map $g \mapsto X$ determines a representation (φ,V) of G. Another representation (φ',V) is defined by the map $g \mapsto Z$ where $Z|j\rangle = w^j|j\rangle$ for a primitive d-th root of unity.

The two representations defined above are essentially equivalent, as they both capture the same group structure through different linear operators on the same vector space. We formalize this definition below.

[5] Throughout these notes, let $\mathbb{F}$ denote $\mathbb{R}$ or $\mathbb{C}$

Definition 14 (Isomorphism of Representations). Two representations (φ, V) and (φ', V') of a group G are said to be *isomorphic* if there exists an invertible linear map (an *isomorphism*) $\psi : V \to V'$ such that

$$\varphi'(g) = \psi \circ \varphi(g) \circ \psi^{-1} \quad \text{for all } g \in G.$$

For example, the operator X corresponding to the shift $|i\rangle \mapsto |[i-1](\bmod d)\rangle$ has eigenvalues $e^{2\pi ik/d}$ for $k = 0, 1, \ldots, d-1$. Hence, if $w = e^{2\pi i/d}$, a primitive root of unity, then the unitary U diagonalizing X satisfies

$$\varphi' = U \circ \varphi \circ U^{\dagger}.$$

Example 5. The *trivial* representation: $\varphi(g) = \mathbb{1}_{\mathbb{F}}$ for all $g \in G$.

Example 6. The *regular* representation of a finite group G: Let $n = |G|$ and $V \cong \mathbb{C}^n$ with basis $\{|g\rangle\}_{g \in G}$, then the linear extension of the map $\varphi(g) : |h\rangle \mapsto |gh\rangle$ to all of V is called the regular representation of G.

Conversely, let (ψ, W) be a representation such that there exists a $w \in W$ so that $\{\psi(g)(w)\}_{g \in G}$ is a basis for W. Then, ψ is isomorphic to the regular representation.

Example 7. The *permutation* representation: Let X be a finite set and G be a group acting on X. Consider the free vector space generated by X, $V \cong \mathbb{C}^m$, where $m = |X|$ and $\{|x\rangle\}_{x \in X}$ is a basis for V. The linear extension of the map $\varphi(g) : |k\rangle \mapsto |gx\rangle$ is the permutation representation of G on V.

2.2 Motivation from Entanglement

We showed in §1.3 that there are efficient ways to detect entanglement in quantum states, for example via the PPT criterion. But such separability criteria are only necessary, not sufficient, and there are known constructions of entangled states that are not detected by the PPT criterion. The problem of deciding separability may become easier when we have additonal information about the states in question. In particular, the presence of symmetries can greatly simplify the structure of quantum states. [6]

We motivate this transition with a well-known class of quantum states known as *Werner states* [7]. Werner introduced this class of states to study hidden variable models in quantum mechanics, as their entanglement properties are easier to analyze than that of general density operators. Consider the state ρ_{AB} on $\mathbb{C}^2 \otimes \mathbb{C}^2$ satisfying the following symmetry property:

$$\rho_{AB} = (U \otimes U)\, \rho_{AB}\, (U \otimes U)^{\dagger}, \quad \textit{for all } U \in \mathcal{U}_2. \tag{4}$$

Here, $\mathcal{U}_2 = \{U \in \mathcal{L}(\mathbb{C}^2) : U^{\dagger}U = \mathbb{1}\}$ is the group of unitaries on $\mathbb{C}^2$. From (4), we can see that ρ_{AB} is invariant under coordinated local basis transformations on each qubit. Many quantum information processing tasks are invariant under such transformations, and we can often assume (4) to be true without loss of generality.

[6] Reducing the complexity of an object with symmetries is a crucial tool in the study of mathematical physics.

[7] See [Wer89] for the original paper.

The symmetry property is powerful, as it eliminates most degrees of freedon for bipartite states. We will later prove this for arbitrary d, but for now, Werner states have the following form:

Proposition 6 (Two-Qubit Werner States). Every quantum state ρ_{AB} on $\mathbb{C}^2 \otimes \mathbb{C}^2$ satisfying (4) is of the form

$$\rho_{AB} = \frac{2-x}{6}\mathbb{1}_{AB} + \frac{2x-1}{6}\mathbb{F}_{AB}, \tag{5}$$

for some parameter $x \in [-1, 1]$.

Proof. Later, we'll develop the representation-theoretic methods to prove this for Werner states on $\mathbb{C}^d \otimes \mathbb{C}^d$. □

There is, however, a simple way of "inferring" the special form of Equation (5) from the unitary invariance of $U^{\otimes 2}\rho_{AB}U^{\otimes 2\dagger} = \rho_{AB}$ by making choices about the unitary U and tracking coefficients on ρ_{AB}. This is completed in Exercise 1.

3 Symmetry & Unitary Representations

4 The Schur-Weyl Duality

5 Werner & Isotropic States

6 Permutation Invariance & de Finetti Theorems

7 Quantum Type Theory

8 Spectrum Estimation

9 Approximate Cloning

10 Universal Source Compression

References

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states: Operational meanings and generalized entropic characterizations. *arXiv preprint quant-ph/9712042*, 1999.

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1–2):1–8, November 1996.

[Wer89] Reinhard F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, 1989.

A Exercises

Exercise 1. *Explicit form of two-qubit Werner states.* Recall the Bell basis

$$\mathfrak{B} = \left\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\right\}, \tag{6}$$

from Remark 1. Consider the following single-qubit unitaries:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{7}$$

(a) Show that $U \otimes U$ for $U \in \{X, Z, H, S\}$ has the following matrix representation in the Bell basis $\mathfrak{B}$:

$$[X \otimes X]_{\mathfrak{B}} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & -1 \end{pmatrix}, \quad [Z \otimes Z]_{\mathfrak{B}} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & -1 \end{pmatrix}, \tag{8}$$

$$[H \otimes H]_{\mathfrak{B}} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 \end{pmatrix}, \quad [S \otimes S]_{\mathfrak{B}} = \begin{pmatrix} \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & i & \cdot \\ \cdot & \cdot & \cdot & i \end{pmatrix}. \tag{9}$$

(Hint: First, determine the action of the unitaries on the computational basis $\{|0\rangle, |1\rangle\}$*.)*

(b) Use part (a) and the relation $(U \otimes U)\rho_{AB}(U \otimes U)^\dagger$ for all U to show that $\rho_{AB} = \alpha \mathbb{1}_{AB} + \beta \mathbb{F}_{AB}$ for some $\alpha, \beta \in \mathbb{C}$. *(Hint: Consider the action of the unitaries on the Bell basis* $\mathfrak{B}$*.)*