An Introduction to Quantum Entanglement

Ion Nechita

March 29, 2020

Contents

Version history

- ver. 0.1 (02/03/2020): basic topics of Lectures 1,2, and a bit of Lecture 3
- ver. 0.2 (09/03/2020): taken out random states and multipartite entanglement of Lectures 2 and 3; these topics will be discussed in separate lectures. Lecture 3 finished. Lecture plan definitive.
- ver. 0.3 (16/03/2020) Chapter on quantum channels finished, minus some proof details
- ver. 0.4 (18/03/2020) Chapter on entanglement criteria and witnesses finished
- ver. 0.5 (23/03/2020) Chapter on random states finished
- ver. 0.6 (29/03/2020) Chapter on multipartite entanglement finished

Introduction

Entanglement is one of the key features in quantum theory, marking a departure form the classical world.

A very comprehensive review on quantum entanglement is [HHHH09].

Chapter 1

Review of linear algebra and basics of QIT

1.1 Axioms of quantum mechanics

We shall start with a brief overview of quantum mechanics from the perspective of quantum information theory. The emphasis will be different than the one in most physics lectures on the topic. In quantum information theory, we shall mostly be dealing with quantum systems having a finite number of degrees of freedom.

We shall start the presentation with the formalism of *pure quantum states*, which is very well adapted to *closed quantum systems*. Later, we shall see that the introduction of *mixed quantum states* is necessary to take into account *open quantum systems*, that is systems in contact with an environment which we do not wish to describe.

Axiom 1.1.1. *To every quantum system A, we associate a finite dimensional, complex Hilbert space $\mathcal{H}_A = \mathbb{C}^d$.*

A *qubit* is a systems having only 2 degrees of freedom, having thus associated the 2-dimensional Hilbert space $\mathbb{C}^2$.

Axiom 1.1.2. *The state of a quantum system A is a unit vector $|\psi\rangle \in \mathcal{H}_A$.*

In the case of the qubit, we have a distinguished basis of $\mathbb{C}^2$, denoted by $\{|0\rangle, |1\rangle\}$, corresponding to the classical bits $0, 1$. An arbitrary quantum state can be thus represented as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$.

Axiom 1.1.3. *The time evolution of a quantum state is governed by a unitary operator acting on its Hilbert space: $|\psi'\rangle = U|\psi\rangle$.*

Axiom 1.1.4. *The measurement of a quantum systems is described by a set of orthogonal projections $\{P_1, \ldots, P_m\}$ acting on $\mathcal{H}$, and summing up to the identity. If a system in the state $|\psi\rangle$ is measured, one obtains the result i with probability $\|P_i|\psi\rangle\|^2$, and the state of the system after the measurement is $|\psi'\rangle = P_i|\psi\rangle / \|P_i|\psi\rangle\|$.*

The following axiom is central to the topic of this lecture.

Axiom 1.1.5. *Given two quantum systems A, B described respectively by Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, the joint Hilbert space of the composed quantum system AB is the* tensor product *$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.*

For example, the most general quantum state of 2 qubits can be described as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{00}|11\rangle,$$

where we write $|ij\rangle := |i\rangle \otimes |j\rangle$ and α_{ij} are complex numbers satisfying $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

The axiom above is to be compared with its counterpart in classical mechanics, where one considers the *Cartesian product* of the respective phase spaces.

When one wants to describe a system A which is part of a composite system AB without making any reference of the system B, a more general formalism is needed, that of *mixed quantum states*. Mathematically, the latter formalism is more pleasant, since the state space is *convex*. The following set of axioms supersede those introduced previously, which can be seen as special cases.

Axiom 1.1.6. *The state of a quantum system A is* unit trace, positive semidefinite *operator ρ acting on $\mathcal{H}_A$.*

Recall that the set of positive semidefinite operators acting on a Hilbert space $\mathcal{H} = \mathbb{C}^d$ is denoted by $\mathcal{PSD}_d$ and is characterized by one of the following equivalent properties:

1. $X \in \mathcal{PSD}_d$ if and only if the spectrum of X is real (i.e. $X = X^*$) and non-negative
2. $X \in \mathcal{PSD}_d$ if and only if $\langle x, Xx\rangle \geq 0$, for all $x \in \mathbb{C}^d$
3. $X = YY^*$, from some $n \times p$ matrix Y; p can be chosen to be the rank of X.

We shall denote by $\mathcal{M}_d^{1,+}$ the set of states of a d-dimensional quantum system:

$$\mathcal{M}_d^{1,+} := \{\rho \in \mathcal{M}_d(\mathbb{C}) \,:\, \rho \geq 0 \text{ and } \operatorname{Tr} \rho = 1\}.$$

In the case $d = 2$, the set of mixed quantum states is particularly nice: it is isomorphic to the unit ball in $\mathbb{R}^3$. Indeed, any quantum state of a qubit can be written as

$$\rho = \frac{1}{2}(I_2 + r_1\sigma_X + r_2\sigma_Y + r_3\sigma_Z),$$

where

$$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

are the Pauli matrices and $r \in \mathbb{R}^3$ is a vector with $\|r\| \leq 1$. It is a fundamental fact that the set $\mathcal{M}_d^{1,+}$ is convex.

Lemma 1.1.7. *The extremal points of $\mathcal{M}_d^{1,+}$ is the set of rank-one projections $|\psi\rangle\langle\psi|$, called* pure quantum states*.*

Hence, the pure-state formalism of quantum mechanics is special case of the mixed-state formalism.

Axiom 1.1.8. *The time evolution of a mixed quantum state is governed by a unitary operator acting on its Hilbert space: $\rho' = U\rho U'$.*

In the axiom above, we assume that the quantum system is isolated from its environment; we shall see in Chapter 4 how quantum systems evolve when in contact with an auxiliary system.

Axiom 1.1.9. *The measurement of a quantum systems is described by a set of positive semidefinite operators $\{M_1, \ldots, M_m\}$ acting on $\mathcal{H}$, and summing up to the identity. If a system in the state ρ is measured, one obtains the result i with probability $\operatorname{Tr}(M_i\rho)$. The tuple $M = (M_1, \ldots, M_m)$ is called a* positive-operator valued measure*, or a POVM.*

The more general formalism of mixed states allows to define a state ρ_A of the A-part of a composite system AB, when the global state of AB is ρ_{AB}. Assume one wants to perform a POVM measurement M on the system A alone; this amounts to measuring $M \otimes I_B = (M_1 \otimes I_B, \ldots, M_m \otimes I_d)$ on the bipartite system AB. Hence, the probability of obtaining outcome i is

$$\mathbb{P}[i] = \mathrm{Tr}[(M_i \otimes I_B)\rho_{AB}] = \mathrm{Tr}[M_i \rho_A], \tag{1.1}$$

where ρ_A is the *reduced state* of ρ_{AB} on subsystem A and can be obtained with the help of the *partial trace*:

$$\rho_A := [\mathrm{id}_A \otimes \mathrm{Tr}_B](\rho_A B) = \mathrm{Tr}_B(\rho_{AB}).$$

Remember that the partial trace operation is defined on simple tensors as

$$\mathrm{Tr}_B(X_A \otimes Y_B) = X_A \operatorname{Tr} Y_B,$$

or, equivalently, by $X_A = \operatorname{Tr}_B X_{AB}$ if and only if, for all Y_B,

$$\mathrm{Tr}[X_{AB}(Y_A \otimes I_B)] = \mathrm{Tr}[X_A Y_A].$$

The upshot is that, in eq. (1.1), the probability of obtaining outcome i when measuring the POVM M on system A alone is expressed as a function of M and of ρ_A, an object which does not involve the system B.

1.2 Graphical notation

Describe graphical notation for

1. vectors
2. linear forms
3. scalar
4. matrices
5. ket-bra, identity
6. 2-tensors
7. tensor product
8. multi-linear maps
9. scalar product (tensor contraction); canonical
10. product of linear maps
11. partial product of multi-linear maps
12. trace
13. partial trace
14. trace is cyclic
15. partial trace lemmas ($A \otimes I \cdot B =$ A partial trace B)
16. vectorization; inverse vectorization
17. vec(AXB) = ***

1.3 Simulation of quantum algorithms using Quirk

Quirk `https://algassert.com/quirk` is a drag-and-drop quantum simulator which can be used to understand the theory behind many quantum protocols and algorithms. In particular, it has very nice integrated visualization methods for multi-qubit quantum states and allows to define custom quantum gates (unitary operators).

Chapter 2

Quantum entanglement: pure states

We introduce in this chapter the notion of *quantum entanglement*, both in the pure and in the mixed state setting, focusing mainly on two quantum systems. As we shall see, the problem of pure bipartite entanglement is perfectly understood thanks to the SVD, while the mixed case is more complicated.

2.1 Pure state entanglement

Entanglement theory is much simpler in the case of pure states (at the level of vectors in Hilbert space) than for mixed quantum states (density matrices). We discuss here the theory for bipartite systems in detail, and mention briefly the multipartite setting; see Chapter **??** for more results in the multipartite case.

Remarkably, quantum entanglement is defined by what it is not: separability. This choice is motivated by the nicer structure of the set of separable states.

Definition 2.1.1. *A pure state $|\varphi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is called* separable *if it can be decomposed as a tensor product*

$$|\varphi\rangle = |x\rangle \otimes |y\rangle. \tag{2.1}$$

for pure quantum states $|x\rangle \in \mathbb{C}^{d_1}$ and $|y\rangle \in \mathbb{C}^{d_2}$. Non-separable states are called entangled.

Diagrammatically, separability of pure states (vectors) amounts to a disconnected diagram, see Figure 2.1a.

(a) A separable state (b) A maximally entangled state

Figure 2.1: Pure state separability vs. entanglement.

Example 2.1.2. *The following two qubit states are separable*

$$|\varphi\rangle = |00\rangle = |0\rangle \otimes |0\rangle \tag{2.2}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{2.3}$$

The state of a pair of electrons emitted from an event which conserves angular momentum is called a singlet state *and is entangled:*

$$|\chi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle). \tag{2.4}$$

The singlet state defined above is an example of a maximally entangled state. This is a 2-qubit maximally entangled state in Quirk, creating using a Hadamard gate and a CNOT gate: [https://algassert.com/quirk#circuit={%22cols%22:[[%22H%22],[%22%E2%80%A2%22,%22X%22]]}]. Note that the 2-qubit CNOT gate is necessary in order to create entanglement between the two qubits in the circuit.

Definition 2.1.3. *The d-dimensional (standard)* maximally entangled *(pure)* state *is the state*

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle. \tag{2.5}$$

More generally, a maximally entangled state in $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is a state of the form

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |e_i\rangle \otimes |f_i\rangle, \tag{2.6}$$

where $d = \min(d_1, d_2)$ and $\{e_1, \ldots, e_d\}$ (resp. $\{f_1, \ldots, f_d\}$) is an orthonormal family of vectors from $\mathbb{C}^{d_1}$ (resp. $\mathbb{C}^{d_2}$).

Pictorially, a maximally entangled state is depicted by a single wire connecting two vector-type labels (up to a normalization), see Figure 2.1b.

2.2 Schmidt decomposition

In many branches of science, decomposing an object in simpler constituent parts is a central theme. In linear algebra, decompositions of operators as products of structured parts is very useful.

Theorem 2.2.1. *Let $X \in \mathcal{M}_{d_1 \times d_2}(\mathbb{C})$ an operator of rank r. Then, there exist non-negative numbers $s_1, \ldots, s_r$ and two isometries $U : \mathbb{C}^r \to \mathbb{C}^{d_1}$, $V : \mathbb{C}^r \to \mathbb{C}^{d_2}$, such that*

$$X = U \operatorname{diag}(s) V^*.$$

Let $X = X^* \in \mathcal{M}_d(\mathbb{C})$ a Hermitian operator of rank r. Then, there exist real numbers $\lambda_1, \ldots, \lambda_r$ and an isometry $V : \mathbb{C}^r \to \mathbb{C}^d$, such that

$$X = V \operatorname{diag}(\lambda) V^*.$$

In this case, we have $s_i = |\lambda_i|$.

2.3 Measure of entanglement

The entanglement of a bipartite pure state is readily characterized in terms of the Schmidt coefficients of the state: a state $|\varphi\rangle$ is separable iff its Schmidt coefficients are $(1, 0, 0, \ldots)$. Not only does the Schmidt decomposition (or the SVD) characterizes qualitatively entanglement, it also gives the canonical quantitative entanglement measure for pure states.

Definition 2.3.1. *The* entropy of entanglement *of a pure state $|\varphi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is the Shannon entropy of its Schmidt coefficients:*

$$E(|\varphi\rangle) = S(\lambda) = -\sum_i \lambda_i \log \lambda_i, \tag{2.7}$$

with

$$|\varphi\rangle = \sum_{i=1}^{\min(d_1,d_2)} \sqrt{\lambda_i} |e_i\rangle \otimes |f_i\rangle. \tag{2.8}$$

Proposition 2.3.2. *The entropy of entanglement of a pure state $|\varphi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is a real number between 0 and $\log \min(d_1, d_2)$. $E(|\varphi\rangle)$ is zero iff $|\varphi\rangle$ is separable. $E(|\varphi\rangle)$ is maximal iff $|\varphi\rangle$ is maximally entangled, in the sense of eq. (2.6).*

It is important to note at this point that computing the Schmidt (or singular value) decomposition of a quantum state is efficient, having $O(d^3)$ complexity for a $d \times d$ matrix (or a quantum state in $\mathbb{C}^d \otimes \mathbb{C}^d$).

2.4 Quantum teleportation

Quantum teleportation is one of the first and most important quantum protocols, discovered by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters in 1993 [].

The goal is to *transmit 1 bit of quantum information* using the following ressources:

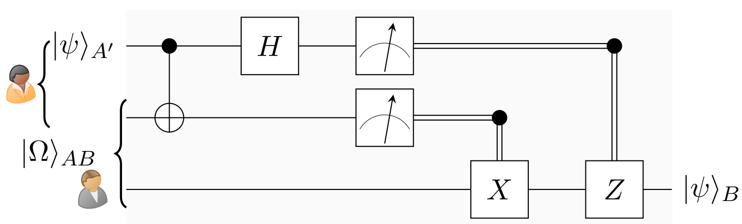
- 2 bits of classical information
- 1 bit of shared quantum entanglement

The interest of this protocol comes from the fact that the shared bit of entanglement could have been set up earlier in the past, and used when convenient. This is one instance where entanglement can be seen as a resource for a protocol. One such scenario could be that Alice and Bob were, at some point in the past, in the same laboratory and created a pair of maximally entangled qubits. They were then separated, each keeping one of the two entangled qubits.

More precisely, Alice wants to transmit to Bob an unknown quantum state $|\psi\rangle \in \mathbb{C}^2$. They only have access to *classical communication* and to a *shared Bell state* $|\Omega\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2} \in \mathbb{C}^4$.

$\boxed{H}$ is the Hadamard gate $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} / \sqrt{2}$. $\boxed{X}$, $\boxed{Z}$ are Pauli matrices. The double line on top signifies that they are *controlled* by a classical bit: the actual gate applied is G^b, where b is the control bit. $\oplus$ is the NOT gate, here controlled by a quantum bit:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$



1. The system starts in the state $|\psi\rangle_{A'} \otimes |\Omega\rangle_{AB}$
2. Alice performs a CNOT operation on her 2 qubits, followed by a Hadamard gate on her A' qubit.
3. Alice *measures* her two qubits in the computational basis $\{|0\rangle, |1\rangle\}$.
4. Alice transmits the *classical* outcomes of her measurements to Bob.
5. Bob performs a controlled σ_X, followed by a controlled σ_Z gate on his qubit.

Theorem 2.4.1. *At the end of the teleportation protocol, with probability 1, Bob's qubit is in the state $|\psi\rangle$.*

Below is the evolution of the joint system, in one of the four possible cases depending on the measurement outcomes:

$$
\begin{aligned}
&(\overbrace{\alpha|0\rangle + \beta|1\rangle}^{|\psi\rangle})_{A'} \otimes (\overbrace{|00\rangle + |11\rangle}^{\sim|\Omega\rangle})_{AB} = \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle \\
&\xrightarrow{\text{CNOT}_{A'A}} \alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle \\
&\xrightarrow{H_{A'}} \alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle \\
&\xrightarrow{\text{measure } A'\text{, outcome } 0} \alpha|000\rangle + \alpha|011\rangle + \beta|010\rangle + \beta|001\rangle \\
&\xrightarrow{\text{measure } A\text{, outcome } 1} \alpha|011\rangle + \beta|010\rangle = |01\rangle_{A'A}(\alpha|1\rangle + \beta|0\rangle)_B \\
&\xrightarrow{X_B^1\text{, then } Z_B^0} |01\rangle_{A'A}(\alpha|0\rangle + \beta|1\rangle)_B = |01\rangle_{A'A}|\psi\rangle_B
\end{aligned}
$$

It is interesting to notice that, at the end of the protocol, the shared entanglement was destroyed, Alice's and Bob's system being now in a product state.

Chapter 3

Quantum entanglement: mixed states

It is important to note at this point that both sets of classical and quantum states (see Figure 3.1) are slices (with the affine hyperplane corresponding to $\sum_i p_i = 1$, resp. $\operatorname{Tr}\rho = 1$) of two cones: the positive quadrant, resp. the positive semidefinite cone:

$$\mathbb{R}^d_+ = \{p \in \mathbb{R}^d \, : \, p_i \geq 0 \, \forall i \in [d]\} \quad \text{and} \quad \mathcal{PSD}_d = \{X \in \mathcal{M}_d^{sa} \, : \, \operatorname{spec} X \subseteq \mathbb{R}_+\}. \tag{3.1}$$

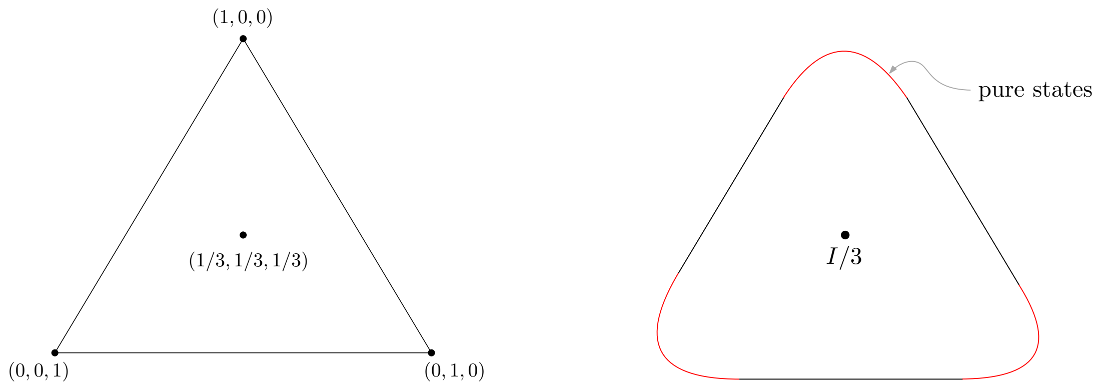


Figure 3.1: Classical (left) and quantum (right) state space.

One is led to consider physical theories corresponding to other cones (encoding different notions of positivity), called *generalized probabilistic theories* (GPTs). This is a very active field of research, see [Lam18] for an excellent introduction to the subject. The classical theory (corresponding to the simplex state space and the cone $\mathbb{R}^d_+$) plays a very special role: entanglement exists in the tensor product of two GPTs if and only if both are non-classical [ALP+19, ALPP19].

3.1 Purification

We have seen that any pure quantum state $|\varphi\rangle \in \mathbb{C}^d$ is associated to a mixed quantum state of the same dimension $\rho = |\varphi\rangle\langle\varphi| \in \mathcal{M}_d^{1,+}$. In order to go from mixed states to pure states, we employ a very useful trick called purification.

Definition 3.1.1. *Let $\rho \in \mathcal{M}_d^{1,+}$ be a mixed quantum state. A unit vector $z \in \mathbb{C}^d \otimes \mathbb{C}^D$ is called a* purification *of ρ if $\rho = \operatorname{Tr}_D |z\rangle\langle z|$.*

For example, for any unit vectors $x \in \mathbb{C}^d$ and $y \in \mathbb{C}^D$, $z = x \otimes y$ is a purification of $\rho = |x\rangle\langle x|$. Recall that the maximally entangled state $\Omega \in \mathbb{C}^d \otimes \mathbb{C}^d$ has maximally mixed reduced density matrices. Hence, Ω is a purification of $\rho = I/d$:

$$\frac{I_d}{d} = [\mathrm{id} \otimes \mathrm{Tr}](\omega), \tag{3.2}$$

where we denote $\omega := |\Omega\rangle\langle\Omega|$.

The following result completely characterizes the existence of purifications.

Proposition 3.1.2. *For a quantum state $\rho \in \mathcal{M}_d^{1,+}$, there exists a purification $z \in \mathbb{C}^d \otimes \mathbb{C}^D$ of ρ if and only if $D \geq \operatorname{rank} \rho$.*

Proof. For the first direction, let us start from the spectral decomposition of ρ:

$$\rho = \sum_{i=1}^{r} \lambda_i |\varphi_i\rangle\langle\varphi_i|, \tag{3.3}$$

where $\lambda_1, \ldots, \lambda_r$ are the eigenvalues of ρ (hence $\lambda_i \geq 0$ and $\sum_{i=1}^r \lambda_i = 1$) and φ_i are orthonormal vectors in $\mathbb{C}^d$. Define the vector

$$\mathbb{C}^d \otimes \mathbb{C}^r \ni z := \sum_{i=1}^{r} \sqrt{\lambda_i} \varphi_i \otimes e_i, \tag{3.4}$$

where $\{e_1, \ldots, e_r\}$ is an orthonormal basis of $\mathbb{C}^r$. Since the vectors φ_i and e_i are orthnormal, the vector z has norm

$$\|z\|^2 = \sum_{i=1}^{r} |\sqrt{\lambda_i}|^2 = 1. \tag{3.5}$$

Let us compute the reduced density matrix of $|z\rangle\langle z|$:

$$\mathrm{Tr}_D |z\rangle\langle z| = \mathrm{Tr}_D \sum_{i,j=1}^{r} \sqrt{\lambda_i \lambda_j} |\varphi_i\rangle\langle\varphi_j| \otimes |e_i\rangle\langle e_j| = \sum_{i,j=1}^{r} \sqrt{\lambda_i \lambda_j} |\varphi_i\rangle\langle\varphi_j| \langle e_i, e_j\rangle = \sum_{i=1}^{r} \lambda_i |\varphi_i\rangle\langle\varphi_i| = \rho, \tag{3.6}$$

proving one implication. For the reverse implication, consider $z \in \mathbb{C}^d \otimes \mathbb{C}^D$ a purification of ρ, and let $Z := \mathrm{vec}^{-1}(z) \in \mathcal{M}_{d \times D}$ its inverse vectorization. Using ***, we have

$$\rho = \mathrm{Tr}_D |z\rangle\langle z| = ZZ^*, \tag{3.7}$$

showing that $D \geq \operatorname{rank} \rho$. □

It is important to notice the relation between the eigenvalue decomposition of a quantum state ρ and the Schmidt decomposition of its purifications z. The degree in which purifications are unique is characterized in the following proposition.

Proposition 3.1.3. *Given a quantum state $\rho \in \mathcal{M}_d^{1,+}$ and purifications $z, w \in \mathbb{C}^d \otimes \mathbb{C}^D$ of ρ, there exists a unitary matrix $U \in \mathcal{U}_D$ such that*

$$w = (I_d \otimes U) z. \tag{3.8}$$

Proof. Let $r = \operatorname{rank} \rho$ and recall that all $d \times D$ purifications of ρ are of the form:

$$z = \sum_{i=1}^{r} \sqrt{\lambda_i} \varphi_i \otimes e_i \tag{3.9}$$

$$w = \sum_{i=1}^{r} \sqrt{\lambda_i} \varphi_i \otimes f_i, \tag{3.10}$$

where $\rho = \sum_{i=1}^{r} \lambda_i |\varphi_i\rangle\langle\varphi_i|$ is the spectral decomposition of ρ and $\{e_i\}$, $\{f_i\}$ are orthonormal families of vectors from $\mathbb{C}^D$. Construct the unitary operator U satisfying

$$Ue_i = f_i \qquad \forall i \in [r]. \tag{3.11}$$

□

Corollary 3.1.4. *All purifications of a pure state $|x\rangle\langle x|$ are of the form $z = x \otimes y$ for some unit vector $y \in \mathbb{C}^D$.*

3.2 Mixed state entanglement

Since the set of mixed quantum states has a convex structure, one is lead to put the same convex structure on the set of separable state, see Figure 3.2.

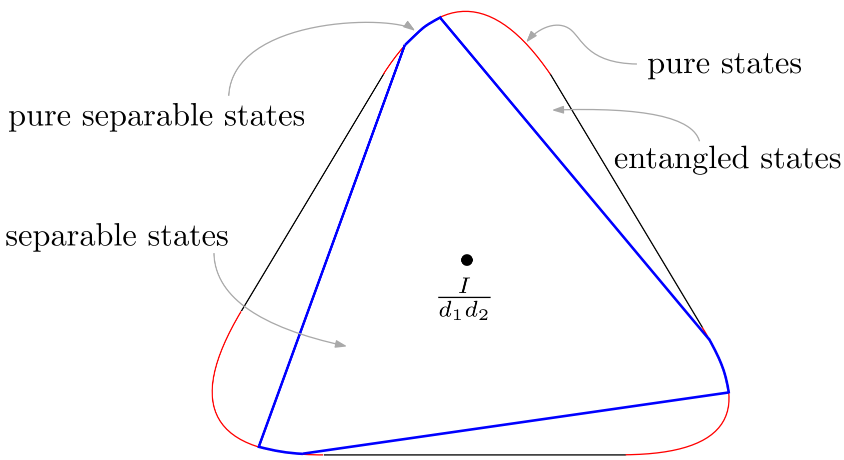


Figure 3.2: Separable states form a convex subset of the set of mixed quantum states.

Definition 3.2.1. *The set of* separable *quantum states in $\mathcal{M}_{d_1} \otimes \mathcal{M}_{d_2}$ is defined to be*

$$\mathcal{SEP}(d_1 : d_2) := \mathrm{conv}\{\rho_1 \otimes \rho_2 \; : \; \rho_i \in \mathcal{M}_{d_i}^{1,+}, \; i = 1, 2\}. \tag{3.12}$$

A non-separable quantum state $\rho \in \mathcal{M}_{d_1 d_2}^{1,+} \setminus \mathcal{SEP}(d_1 : d_2)$ is called entangled.

From a physical point of view, separable states are the ones two distant parties, Alice and Bob, can prepare locally using shared randomness: Alice and Bob can prepare

$$\rho^{AB} = \sum_{i=1}^{r} p_i \rho_i^A \otimes \rho_i^B \tag{3.13}$$

by selecting with probability p_i the local (product) state $\rho_i^A \otimes \rho_i^B$. Contrary to pure states, there exist mixed separable quantum states which are not tensor products (i.e. the sum above has more than 1 term).

Note that the set of separable states is described via its extreme points.

Lemma 3.2.2. *The extreme point of the set of mixed separable quantum states are pure separable states:*

$$\mathrm{ext}\, \mathcal{SEP}(d_1 : d_2) = \{|x\rangle\langle x| \otimes |y\rangle\langle y|\}. \tag{3.14}$$

Proof. The statement follows from the spectral decomposition of the states $\rho_i^{A,B}$ from eq. (3.13):

$$\rho^{AB} = \sum_{i=1}^{r} \sum_{a=1}^{d_1} \sum_{b=1}^{d_2} p_i \lambda_a \mu_b |x_{i,a}\rangle\langle x_{i,a}| \otimes |y_{i,b}\rangle\langle y_{i,b}|. \tag{3.15}$$

□

In particular, a pure quantum state $\rho = |z\rangle\langle z|$ is separable if and only if $z = x \otimes y$ and thus $\rho = |x\rangle\langle x| \otimes |y\rangle\langle y|$.

The exists one situation in which the separability of mixed states is easy to understand.

Proposition 3.2.3. *Let ρ_{AB} a mixed bypartite quantum state with the property that the partial trace $\rho_A := \operatorname{Tr}_B \rho_{AB}$ is pure. Then, ρ is a product state (hence separable): $\rho = \rho_A \otimes \rho_B$.*

Proof. Consider a the spectral decomposition of ρ:

$$\rho = \sum_{i=1}^{r} \lambda_i |\varphi_i\rangle\langle\varphi_i|, \tag{3.16}$$

where $\varphi_i \in \mathbb{C}^A \otimes \mathbb{C}^B$ are orthonormal states. We have

$$\rho_A = \sum_{i=1}^{r} \lambda_i \operatorname{Tr}_B |\varphi_i\rangle\langle\varphi_i|. \tag{3.17}$$

Since $\rho_A = |x\rangle\langle x|$ is pure (and thus an extremal point of $\mathcal{M}_A^{1,+}$), it must be that each of the density matrices $\operatorname{Tr}_B |\varphi_i\rangle\langle\varphi_i|$ must be equal to ρ_A. In turn, this implies, using Corollary 3.1.4, that $\varphi_i = x \otimes y_i$. We obtain

$$\rho = |x\rangle\langle x| \otimes \left(\sum_{i=1}^{r} \lambda_i |y_i\rangle\langle y_i| \right), \tag{3.18}$$

proving the claim. □

The following remarkable result is due to Gurvits and Barnum; it is a striking result about the geometry of the set of (separable) quantum states. For the proof, see, e.g., [AS17, Theorem 9.15 or Exercise 9.8].

Theorem 3.2.4 ([GB02])**.** *The largest euclidean ball, centered at $I/(d_1 d_2)$ and contained in $\mathcal{M}_{d_1 d_2}^{1,+}$ is separable.*

Note that the radius of the largest euclidean ball contained in $\mathcal{M}_D^{1,+}$ is

$$r_{\text{in}} = \frac{1}{\sqrt{D(D-1)}}; \tag{3.19}$$

this is known as the *in-radius* of $\mathcal{M}_D^{1,+}$, see [AS17, Eq. (2.7)]. It is very easy to see that the *out-radius* of $\mathcal{M}_D^{1,+}$ (i.e. the radius of the smallest ball containing the set) is

$$r_{\text{out}} = \sqrt{\frac{D-1}{D}}. \tag{3.20}$$

Note that in the case $D = 2$ (which is not relevant for entanglement theory), these two radii agree, since the Bloch ball is an euclidean ball. In general, they differ by a factor $D - 1$, which can be seen as a measure of "non-roundness" of the convex body $\mathcal{M}_D^{1,+}$.

Chapter 4

Positive and completely positive maps

The goal of this Chapter is to prove Theorem 4.2.1, characterizing *quantum channels*, the most general physical transformation of quantum states.

4.1 Physical transformations of quantum states

Consider a physical transformation $\Phi : \mathcal{M}_d \to \mathcal{M}_D$, mapping d-dimensional quantum states to D-dimensional quantum states. What is the most general form of such a map? The obvious requirement is that

$$\Phi(\mathcal{M}_d^{1,+}) \subseteq \mathcal{M}_D^{1,+}. \tag{4.1}$$

In other words, Φ must satisfy the following two conditions:

- If $X \in \mathcal{M}_d$ is a positive semidefinite matrix, then so is $\Phi(X) \in \mathcal{M}_D$
- The map Φ must be *trace preserving* (TP): for all $X \in \mathcal{M}_d$,

$$\operatorname{Tr} \Phi(X) = \operatorname{Tr} X. \tag{4.2}$$

Definition 4.1.1. *A linear map $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ is called* positive *if*

$$X \geq 0 \implies \Phi(X) \geq 0. \tag{4.3}$$

Let us consider some simple examples of such maps.

Example 4.1.2. *The following maps are positive and trace preserving (here, $D = d$):*

1. $\Phi(X) = UXU^*$, *for some unitary operator $U \in \mathcal{U}_d$*
2. $\Phi(X) = \operatorname{Tr} X \cdot \frac{I}{d}$
3. $\Phi(X) = \operatorname{diag}(X)$
4. $\Phi(X) = X^\top$, *the* transpose map.

In the simplest case $d = D = 2$, restricting the map to quantum states $\mathcal{M}_2^{1,+}$ yields a very pleasant geometrical interpretation:

$$\Phi(\rho_r) = \rho_{r'}, \tag{4.4}$$

where ρ_r is the Bloch ball state

$$\rho_r = \frac{1}{2}(I_2 + r_1\sigma_X + r_2\sigma_Y + r_3\sigma_Z). \tag{4.5}$$

Note that since the Pauli matrices are traceless, the trace preservation condition is automatically satisfied, while the positivity condition reads $\|r\| \leq 1 \implies \|r'\| \leq 1$. In other words, positive trace preserving qubit maps map the Bloch ball to an ellipsoid *contained* in the Bloch ball. In the examples above, the resulting ellipsoids are, respectively:

1. A rotation of the Bloch ball
2. The center of the Bloch ball (which is a degenerate ellipsoid reduced to a point)
3. The North pole - South pole segment
4. A symmetry with respect to the $X - Z$ plane:

$$r = (r_1, r_2, r_3) \mapsto r' = (r_1, -r_2, r_3). \tag{4.6}$$

Let us see now how entanglement adds extra restrictions to physical maps Φ. Consider the transpose map $\Phi(X) = X^T$ acting on a qubit, and assume that the qubit in question is maximally entangled with another qubit. Applying the map Φ only on the second qubit translates to applying the map $\mathrm{id}_2 \otimes \Phi$ to both qubits, so the resulting quantum state is

$$\rho = [\mathrm{id}_2 \otimes \Phi](\omega), \tag{4.7}$$

where $\omega = |\Omega\rangle\langle\Omega| \in \mathcal{M}_4^{1,+}$ is the maximally entangled density matrix on 2 qubits. We have

$$\omega = \frac{1}{2}\left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) = \frac{1}{2}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}. \tag{4.8}$$

The resulting matrix $\sigma = [\mathrm{id}_2 \otimes \Phi](\omega)$ is called the *partial transposition* of ω. This corresponds to taking the transpose of each block B_{ij}:

$$\sigma = \frac{1}{2}\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right). \tag{4.9}$$

Note that σ is not positive semidefinite! Hence, *the transposition map does not correspond to a valid physical qubit transformation* (the reason for this being entanglement). To deal with this problem, we introduce the following, stronger, positivity notion.

Definition 4.1.3. *A linear map $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ is called* completely positive *if, for all positive integers $N \geq 1$*

$$\mathcal{M}_d \otimes \mathcal{M}_N \ni X \geq 0 \implies [\Phi \otimes \mathrm{id}_N](X) \geq 0. \tag{4.10}$$

It is easy to see that the first three maps in Example 4.1.2 are completely positive. Above, we have shown that the transposition map, although positive, it is not completely positive. This type of linear maps will play an important role in Chapter 5.

It turns out that complete positivity is the right positivity notion needed for quantum mechanics.

Definition 4.1.4. *A linear map $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ is called a* quantum channel *if it is completely positive and trace preserving. Quantum channels are the most general physical transformations of states in quantum mechanics.*

It is easy to check that the composition of two positive (resp. completely positive) maps is positive (resp. completely positive). Complete positivity is also stable by tensor products.

Proposition 4.1.5. *Let $\Phi_{1,2}$ be two quantum channels. Then, so is $\Phi_1 \otimes \Phi_2$.*

Proof. Trace preservation is easily checked, while complete positivity can be shown as follows:

$$\Phi_1 \otimes \Phi_2 \otimes \mathrm{id}_N = [\Phi_1 \otimes \mathrm{id}_{d_2} \otimes \mathrm{id}_N] \circ [\mathrm{id}_{d_1} \otimes \Phi_2 \otimes \mathrm{id}_N]. \tag{4.11}$$

□

To end this section, let us consider the corresponding notions in the classical world, that is for classical states. Remember that classical states are probability vectors, so maps preserving probability vectors are of the form $T : \mathbb{R}^d \to \mathbb{R}^D$ with the following two properties:

- positivity: $T_{ij} \geq 0$, for all $i \in [D]$, $j \in [d]$
- trace preservation: for all $j \in [d]$, $\sum_{i=1}^D T_{ij} = 1$.

Such maps are known in classical probability as *(column-)stochastic matrices* or *Markov maps*. In this case, complete positivity is trivial, since it follows from the usual notion of positivity. This is due to the fact that there is no "classical entanglement", and has a more abstract formulation in operator algebra [Pau02, Theorems 3.9 and 3.11].

4.2 Structure theorem for quantum channels

Before stating Theorem 4.2.1, let us introduce a very important object associated to a linear map $\Phi : \mathcal{M}_d \to \mathcal{M}_D$, it's Choi-Jamiołkowski matrix $J(\Phi)$:

$$\mathcal{M}_D \otimes \mathcal{M}_d \ni J(\Phi) := [\Phi \otimes \mathrm{id}_d](d \cdot \omega_d) = \sum_{i,j=1}^d \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|. \tag{4.12}$$

One can recover the channel Φ from its Choi matrix by the following formula (see also Figure 4.1):

$$\Phi(X) = \mathrm{Tr}_d[J(\Phi) \cdot I_D \otimes X^\top]. \tag{4.13}$$

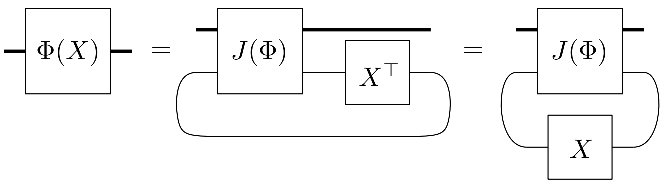


Figure 4.1: Recovering the output $\Phi(X)$ of a quantum channel from its Choi matrix $J(\Phi)$. Strings corresponding to the vector space $\mathbb{C}^D$ are thicker.

Theorem 4.2.1. *Let $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ a linear transformation. The following assertions are equivalent:*

(1) The map Φ is a quantum channel.

(2) The map $\Phi \otimes \mathrm{id}_d$ is positive and trace preserving.

(3) The Choi map $J(\Phi)$ is positive semidefinite and $\mathrm{Tr}_D\, J(\Phi) = I_d$.

(4) The exist R matrices $A_1, \ldots, A_R \in \mathcal{M}_{D\times d}$ such that

$$\Phi(X) = \sum_{i=1}^R A_i X A_i^* \qquad \text{and} \qquad \sum_{i=1}^R A_i^* A_i = I_d. \tag{4.14}$$

(5) There exist some positive integer R and an isometry $V : \mathbb{C}^d \to \mathbb{C}^D \otimes \mathbb{C}^R$ such that

$$\Phi(X) = \mathrm{Tr}_R(VXV^*). \tag{4.15}$$

The decomposition (4) above is known as the Kraus decomposition, *while (5) is know as the* Stinespring dilation *of the channel Φ. The integer R above can be taken to be $R = \operatorname{rank} J(\Phi)$, value which is called the* Choi rank *of Φ.*

Before proving the theorem, let us restate point (5) above in terms closer to open quantum systems theory. Let us consider the case $D = d$. One can see then the isometry V as a truncation of a larger unitary matrix $U \in \mathcal{U}_{dR}$ as follows:

$$Vx = Ux \otimes |\psi\rangle, \tag{4.16}$$

for some unit norm vector $|\psi\rangle$. Then, equation (4.15) reads, for a quantum state ρ as an input:

$$\Phi(\rho) = \mathrm{Tr}_R[U(\rho \otimes |\psi\rangle\langle\psi|)U^*]. \tag{4.17}$$

One can interpret the quantum evolution above as the succession of three steps:

1. The system ρ comes into contact with an environment, which is in a pure state $|\psi\rangle\langle\psi|$.
2. The system and the environment undergo a *global* unitary evolution governed by the joint unitary operator U. This evolution might entangle the two systems.
3. The environment system is traced out.

This type of interaction is paradigmatic in the theory of open quantum systems. However, the more compact form (4.15) is mathematically nicer, since it allows for different input/output dimensions and deals with the freedom in choosing the pair $(U, |\psi\rangle)$.

Proof. The implications (1) $\implies$ (2) $\implies$ (3) are clear. Let us now prove (3) $\implies$ (4). Consider the eigenvalue decomposition of $J(\Phi)$:

$$J(\Phi) = \sum_{r=1}^{R} \lambda_r |a_r\rangle\langle a_r|, \tag{4.18}$$

for non-negative scalars λ_r and orthonormal vectors $a_r \in \mathbb{C}^D \otimes \mathbb{C}^d$. Define $A_i := \sqrt{\lambda_i}\,\mathrm{vec}^{-1}(a_i) \in \mathcal{M}_{D\times d}$. We have then (see Figure 4.2):

$$\Phi(X) = \mathrm{Tr}_D(J(\Phi) \cdot I_D \otimes X^\top) = \sum_{i=1}^{R} \mathrm{Tr}_D(A_i \otimes I_d \cdot d\omega \cdot A_i^* \otimes I_d \cdot I_D \otimes X^\top) = \sum_{i=1}^{R} A_i X A_i^*. \tag{4.19}$$

The formula $\sum_{i=1}^{R} A_i^* A_i$ is obtained as follows:

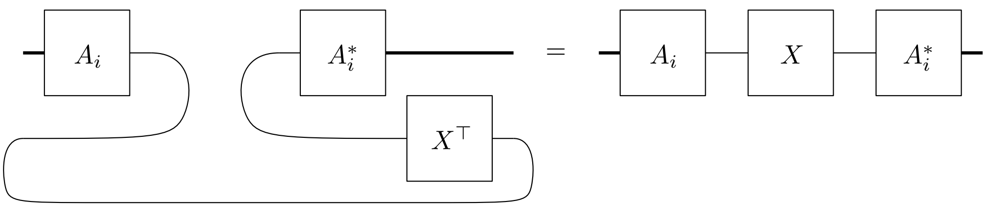


Figure 4.2: Graphical representation of the reduction in formula (4.19).

$$\sum_{i=1}^{R} A_i^* A_i = \sum_{i=1}^{R} \lambda_i (\mathrm{Tr}_D\, |a_i\rangle\langle a_i|)^\top = (\mathrm{Tr}_D\, J(\Phi))^\top = I_d. \tag{4.20}$$

Let us now check (4) $\implies$ (5). Define the operator $V : \mathbb{C}^d \to \mathbb{C}^D \otimes \mathbb{C}^R$ by

$$V = \sum_{i=1}^{R} A_i \otimes |i\rangle, \tag{4.21}$$

where $\{|i\rangle\}_{i=1}^R$ is some fixed orthonormal basis of $\mathbb{C}^R$. We have

$$\mathrm{Tr}_R(VXV^*) = \sum_{i,j=1}^{R} A_i X A_j^* \,\mathrm{Tr}(|i\rangle\langle j|) = \sum_{i=1}^{R} A_i X A_i^* = \Phi(X). \tag{4.22}$$

The fact that V is an isometry ($V^*V = I_d$) follows from the relation $\sum_{i=1}^R A_i^* A_i = I_d$.

Finally, let us prove (5) $\implies$ (1). Fix an integer $N \geq 1$, and a positive semidefinite matrix $X \in (\mathcal{M}_d \otimes \mathcal{M}_N)^+$. We have

$$[\Phi \otimes \mathrm{id}_N](X) = \mathrm{Tr}_R[(V \otimes I_N)X(V \otimes I_N)^*] \geq 0, \tag{4.23}$$

proving that the map $\Phi \otimes \mathrm{id}_N$ is positive, and thus Φ is completely positive. The trace preservation property is trivial.

$\square$

We end this chapter by applying Theorem 4.2.1 to the three quantum channels from Example 4.1.2.

For the unitary conjugation map, one can easily see that the Choi matrix has rank 1

$$J(\Phi) = |(U \otimes I_d)\Omega\rangle\langle(U \otimes I_d)\Omega|, \tag{4.24}$$

and thus both the Kraus decomposition and the Stinespring dilation are trivial.

For the completely depolarzing map, the Choi matrix is

$$J(\Phi) = \frac{1}{d^2} I_{d^2}. \tag{4.25}$$

One can chose

$$A_{ij} = \frac{1}{\sqrt{d}} |i\rangle\langle j| \tag{4.26}$$

for the Kraus operators.

For the diagonal map, suitable Kraus operators are $A_i = |i\rangle\langle i|$, the Choi rank of this matrix being d.

Chapter 5

Positive maps and entanglement criteria

Starting from the example of the transposition map on qubits, we have studied in the previous chapter the notion of positive and completely positive maps. We have seen that the mathematical structure needed to model physical maps is complete positivity, the more general notion of positive linear maps not being sufficient to guarantee positivity of output states (for entangled inputs).

We restate this simple but crucial observation in the following proposition.

Proposition 5.0.1. *If $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ is a* completely positive *linear map and $\rho \in (\mathcal{M}_d \otimes \mathcal{M}_{d'})^{1,+}$ is a bipartite quantum state, then $[\Phi \otimes \mathrm{id}_{d'}](\rho)$ is positive semidefinite.*

If $\Psi : \mathcal{M}_d \to \mathcal{M}_D$ is a positive *(but not necessarily CP) linear map and $\sigma \in (\mathcal{M}_d \otimes \mathcal{M}_{d'})^{1,+}$ is a bipartite* separable *quantum state, then $[\Psi \otimes \mathrm{id}_{d'}](\sigma)$ is positive semidefinite.*

In particular, if $\rho \in (\mathcal{M}_d \otimes \mathcal{M}_{d'})^{1,+}$ is an arbitrary bipartite quantum state, and $\Psi : \mathcal{M}_d \to \mathcal{M}_D$ is a positive linear map, then

$$[\Psi \otimes \mathrm{id}_{d'}](\rho) \ngeq 0 \implies \rho \text{ is entangled.} \tag{5.1}$$

Proof. The only point above needing a proof is the second one. Indeed, since σ is separable, it has a decomposition

$$\sigma = \sum_{i=1}^{R} p_i \alpha_i \otimes \beta_i \tag{5.2}$$

where $p = (p_1, \ldots, p_R)$ is a probability vector and $\alpha_1, \ldots, \alpha_R \in \mathcal{M}_d^{1,+}$, $\beta_1, \ldots, \beta_R \in \mathcal{M}_{d'}^{1,+}$. We have

$$[\Psi \otimes \mathrm{id}_{d'}](\sigma) = \sum_{i=1}^{R} p_i \Psi(\alpha_i) \otimes \beta_i \geq 0, \tag{5.3}$$

since Ψ being positive yields $\alpha_i \geq 0 \implies \Psi(\alpha_i) \geq 0$. □

The third point in the observation above says that any positive (but not completely positive) map gives an *entanglement criterion*: if we apply it to half of a quantum state and we obtain a matrix which is not positive semidefinite, this proves that the quantum state we had was entangled.

Note that, if we use such a positive map and we obtain a positive semidefinite output, then the test is inconclusive: we cannot conclude that the original state was separable. This is in line with the hardness of the separability vs. entanglement problem. If one wants to certify separability, one needs to use *all* positive maps. The following result states that the set of separable states and the set of positive maps are *dual*, see [HHH96] or [AS17, Theorem 2.34].

Theorem 5.0.2. *A quantum state $\rho \in (\mathcal{M}_d \otimes \mathcal{M}_{d'})^{1,+}$ is entangled if and only if there exists a positive map $\Psi : \mathcal{M}_d \to \mathcal{M}_{d'}$ such that*

$$[\Psi \otimes \mathrm{id}_{d'}](\rho) \not\geq 0. \tag{5.4}$$

In the following two sections we shall discuss two very important cases of positive maps which give interesting entanglement criteria: the transposition and the reduction map.

5.1 The partial transposition (PPT) criterion

We have already seen that the transposition map

$$\mathrm{transp} : \mathcal{M}_d \to \mathcal{M}_d \tag{5.5}$$

$$X \mapsto X^\top \tag{5.6}$$

is positive, since it does not change the spectrum of its input. The entanglement criterion given by this positive map is of crucial importance in quantum information theory, historically being also the first one considered (by Peres and the Horodeckis) [Per96, HHH96]. We restate the criterion below.

Definition 5.1.1. *A quantum state $\rho \in \mathcal{M}_{dd'}^{1,+}$ is said to have a positive partial transpose (or to be PPT) if*

$$\rho^\Gamma := [\mathrm{id}_d \otimes \mathrm{transp}_{d'}](\rho) \geq 0. \tag{5.7}$$

The set of PPT states defined by

$$\mathcal{PPT}(d : d') := \{\rho \in \mathcal{M}_{dd'}^{1,+} \; : \; \rho^\Gamma \geq 0\}. \tag{5.8}$$

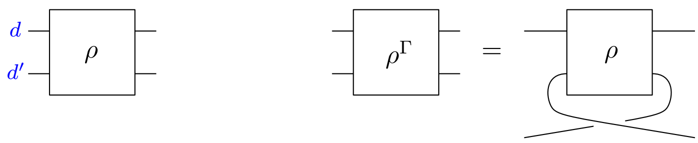


Figure 5.1: A bipartite quantum state and its partial transpose.

It is clear from the definition that $\mathcal{PPT}(d : d')$ is a convex set and that, for all d, d',

$$\mathcal{SEP}(d : d') \subseteq \mathcal{PPT}(d : d'). \tag{5.9}$$

See Figure 5.1 for the difference between a quantum state and it's partial transpose, and Figure 5.2 for the inclusion (5.9). The importance of the PPT criterion stems from the following result, due to Woronowicz [Wor76].

Theorem 5.1.2. *For $(d, d') \in \{(2, 2), (2, 3), (3, 2)\}$, we have*

$$\mathcal{SEP}(d : d') = \mathcal{PPT}(d : d'). \tag{5.10}$$

For larger dimensions (i.e. $dd' > 6$), the inclusion in (5.9) is strict.

Proof. The proof relies on the following result, proven by Woronowicz in [Wor76], which we shall admit:

Any positive map $\Psi : \mathcal{M}_2 \to \mathcal{M}_{2,3}$ can be decomposed as $\Psi = \Phi_1 + \Phi_2 \circ \mathrm{transp}$, where $\Phi_{1,2}$ are completely positive maps.

To prove now the equality case in (5.9), we need to show that every entangled state ρ is dected by the transpose map. Indeed, let Ψ be a positive map detecting ρ. We have

$$0 \not\leq [\mathrm{id}_d \otimes \Psi](\rho) = [\mathrm{id}_d \otimes \Phi_1](\rho) + [\mathrm{id}_d \otimes \Phi_2 \circ \mathrm{transp}](\rho) = [\mathrm{id}_d \otimes \Phi_1](\rho) + [\mathrm{id}_d \otimes \Phi_2](\rho^\Gamma). \tag{5.11}$$

Since $\Phi_{1,2}$ are CP, ρ^Γ cannot be positive semidefinite, proving the claim. $\square$

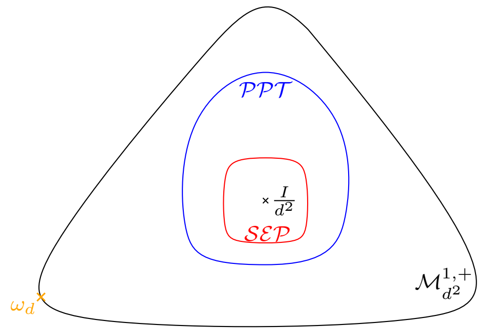


Figure 5.2: The set of all quantum states ($\mathcal{M}_{d^2}^{1,+}$), the set of separable states ($\mathcal{SEP}$) and the PPT set ($\mathcal{PPT}$). Also represented are the maximally mixed state I/d^2 and the maximally entangled state ω_d.

Besides its importance in small dimensions, the PPT criterion detects all entangled *pure* states.

Proposition 5.1.3. *Let $\mathcal{M}_{dd'}^{1,+} \ni \rho = |\psi\rangle\langle\psi|$ be a pure quantum state. Then*

$$\rho \text{ is separable} \iff \rho^\Gamma \geq 0. \tag{5.12}$$

Proof. Let $\psi \in \mathbb{C}^d \otimes \mathbb{C}^d$ be a pure quantum state and consider its Schmidt decomposition:

$$\psi = \sum_{i=1}^R \sqrt{\lambda_i} a_i \otimes b_i, \tag{5.13}$$

for a probability vector $\lambda = (\lambda_1, \ldots, \lambda_R)$ ($R \geq 1$ is the Schmidt rank of ψ) and orthonormal families $\{a_i\}_{i=1}^R$, resp. $\{b_j\}_{j=1}^R$ in $\mathbb{C}^d$. We compute the partial trace

$$|\psi\rangle\langle\psi|^\Gamma = [\mathrm{id}_d \otimes \mathrm{transp}_d]\left(\sum_{i,j=1}^R \sqrt{\lambda_i\lambda_j}|a_i\rangle\langle a_j| \otimes |b_i\rangle\langle b_j|\right) = \sum_{i,j=1}^R \sqrt{\lambda_i\lambda_j}|a_i\rangle\langle a_j| \otimes |\bar b_j\rangle\langle \bar b_i|. \tag{5.14}$$

Note that the matrix $|\psi\rangle\langle\psi|^\Gamma$ is not rank one anymore, see Figure 5.3. It can be readily checked that $|\psi\rangle\langle\psi|^\Gamma$ has the following non-zero eigenvalues and corresponding eigenvectors:

for $1 \leq s = t \leq R$, eigenvalue λ_s with eigenvector $a_s \otimes \bar b_s$

for $1 \leq s < t \leq R$, eigenvalue $\sqrt{\lambda_s\lambda_t}$ with eigenvector $\frac{1}{\sqrt{2}}(a_s \otimes \bar b_t + a_t \otimes \bar b_s)$

for $1 \leq t < s \leq R$, eigenvalue $-\sqrt{\lambda_s\lambda_t}$ with eigenvector $\frac{1}{\sqrt{2}}(a_s \otimes \bar b_t - a_t \otimes \bar b_s)$.

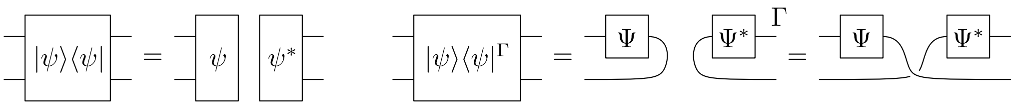


Figure 5.3: A pure bipartite quantum state (left) and its partial transpose (right). The matrix Ψ is the inverse vectorization of the bipartite pure state ψ: $\Psi = \mathrm{vec}^{-1}(\psi)$.

Hence, the matrix $|\psi\rangle\langle\psi|^\Gamma$ is positive semidefinite if and only if $R = 1$, i.e. $|\psi\rangle\langle\psi|$ is separable. □

Finally, let us analyze in detail an example of application of the PPT criterion, in the special case of *isotropic quantum states* of the form

$$\rho_t = t\omega_d + (1-t)\frac{I}{d^2}, \tag{5.15}$$

where $t \in [0,1]$ is a parameter. These states parameterize the segment between the maximally mixed state and the maximally entangled state, see Figure 5.2.

Proposition 5.1.4. *The PPT criterion is exact for isotropic states:*

$$\rho_t \in \mathcal{SEP}(d:d) \iff \rho_t \in \mathcal{PPT}(d:d) \iff t \in [0, 1/(d+1)]. \tag{5.16}$$

Proof. It is clear that $\rho_t \in \mathcal{SEP}(d:d) \implies \rho_t \in \mathcal{PPT}(d:d)$. Let us compute the partial transposition of the quantum state ρ_t:

$$\rho_t^\Gamma = t\omega_d^\Gamma + \frac{1-t}{d^2} I_{d^2}^\Gamma = \frac{t}{d}F_d + \frac{1-t}{d^2} I_{d^2}, \tag{5.17}$$

where $F_d \in \mathcal{U}_{d^2}$ denotes the (unitary) *flip operator*: $F_d x \otimes y = y \otimes x$, for all $x, y \in \mathbb{C}^d$; see Figure 5.4 for the equality $d\omega_d^\Gamma = F_d$. Now, the flip operator is self-adjoint and unitary, so it

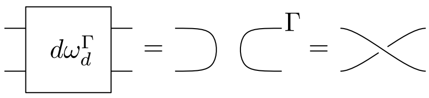


Figure 5.4: The partial transpose of the (rescaled) maximally entangled state is the flip operator.

has eigenvalues ± 1 with eigenspaces given by the symmetric subspace (for eigenvalue $+1$) and the anti-symmetric subspace (for eigenvalue -1) of $\mathbb{C}^d \otimes \mathbb{C}^d$, with respective dimensions

$$\dim \vee^2(\mathbb{C}^d) = \binom{d+1}{2} = \frac{d(d+1)}{2} \qquad \text{and} \qquad \dim \wedge^2(\mathbb{C}^d) = \binom{d}{2} = \frac{d(d-1)}{2}. \tag{5.18}$$

Hence, the matrix from eq. (5.17) is positive semidefinite if and only if

$$-\frac{t}{d} + \frac{1-t}{d^2} \geq 0 \iff t \leq \frac{1}{d+1}, \tag{5.19}$$

proving the second implication.

Let us now consider an isotropic state ρ_t, with $t = 1/(d+1)$ and show that it is separable; it is clear that the separability of ρ_s for smaller values of $s < t$ follows from the one of ρ_t by convexity. We have now

$$\rho_{1/(d+1)} = \int_{x\in\mathbb{C}^d,\, \|x\|=1} |x\rangle\langle x| \otimes |\bar{x}\rangle\langle\bar{x}| \, \mathrm{d}\sigma(x), \tag{5.20}$$

where $\sigma(x)$ is the Lebesgue measure on the unit sphere of the complex Hilbert space $\mathbb{C}^d$. We postpone the proof of this fact to Chapter 6. $\square$

5.2 The reduction criterion

The reduction criterion is another entanglement criterion of significant importance in quantum information theory. The starting point is the following linear map, called the *reduction map*:

$$R : \mathcal{M}_d \to \mathcal{M}_d \tag{5.21}$$
$$X \mapsto (\operatorname{Tr} X) I_d - X. \tag{5.22}$$

We leave the proof of the following fact as an exercise to the reader.

Proposition 5.2.1. *The reduction map is positive.*

The reduction map being positive, we can define the set of quantum states which pass the entanglement test given by this map:

$$\mathcal{RED}(d:d') := \{\rho \in \mathcal{M}_{dd'}^{1,+} \, : \, [\mathrm{id}_d \otimes R_{d'}](\rho) \geq 0\} \tag{5.23}$$
$$= \{\rho_{AB} \in \mathcal{M}_{dd'}^{1,+} \, : \, \rho_A \otimes I_{d'} - \rho_{AB} \geq 0\}. \tag{5.24}$$

As in the case of the partial transposition, we have that the set of reduction-positive states is an upper bound for the set of separable states:

$$\mathcal{SEP}(d:d') \subseteq \mathcal{RED}(d:d'). \tag{5.25}$$

Another similarity between the partial reduction and the partial transposition criteria is the fact that they both detect pure entangled states.

Proposition 5.2.2. *Let $\mathcal{M}_{dd'}^{1,+} \ni \rho = |\psi\rangle\langle\psi|$ be a pure quantum state. Then*

$$\rho \textit{ is separable} \iff [\mathrm{id}_d \otimes R_{d'}](\rho) \geq 0. \tag{5.26}$$

Proof. Let $\rho_{AB} = |\psi\rangle\langle\psi|$ be a pure quantum state for $\psi \in \mathbb{C}^d \otimes \mathbb{C}^{d'}$. We have

$$\langle\psi|\rho_A \otimes I_{d'} - \rho_{AB}|\psi\rangle = \mathrm{Tr}(\rho_A^2) - 1 \tag{5.27}$$

which is non-negative if and only if $\mathrm{Tr}(\rho_A^2) = 1$, that is if ρ_A is also pure, which in turn is equivalent to ρ_{AB} being separable (see Proposition 3.2.3). $\square$

Note that the reduction criterion is *weaker* than the PPT criterion, in the following sense: for a quantum state $\rho \in \mathcal{M}^{1,+}dd'$,

$$[\mathrm{id}_d \otimes R_{d'}](\rho) \ngeq 0 \implies [\mathrm{id}_d \otimes \mathrm{transp}_{d'}](\rho) \ngeq 0, \tag{5.28}$$

meaning that if the reduction criterion detects the entanglement in ρ, then so does the PPT criterion. In other words, the set $\mathcal{PPT}$ is a better approximation to $\mathcal{SEP}$ than $\mathcal{RED}$:

$$\mathcal{SEP}(d:d') \subseteq \mathcal{PPT}(d:d') \subseteq \mathcal{RED}(d:d'). \tag{5.29}$$

These facts follow from the simple observation that the map $R \circ \mathrm{transp}$ is completely positive (we leave the proof as an exercise for the reader). The importance of the reduction criterion in quantum information theory comes from its relation to *entanglement distillation*: any state which violates the reduction criterion is distillable (meaning that one can extract a pure maximally entangled state from it, using local operations and classical communication) [HH99].

Chapter 6

Random quantum states

6.1 Pure states

We discuss now the probability that a randomly chosen quantum state is entangled. This is motivated by the question of *typicality of entanglement*: in which quantum systems (or models) is entanglement typical, and in which systems separability is the norm? We shall focus here exclusively on the bipartite case. The efficiency of several entanglement criteria from the point of view of random states will be discussed in later chapters. add references here to later chapters: PPT, realignment

We start with the case of pure states. First, we have to define what is a random pure state. Since pure quantum states are unit-norm vectors in a finite dimensional Hilbert space, the uniform (Lebesgue) measure on the unit sphere of the Hilbert space is the natural candidate in this setting.

Definition 6.1.1. *A d-dimensional* random pure quantum state *is a random uniform point on the unit sphere of* $\mathbb{C}^d$.

Since the set of separable states corresponds to unit-rank tensors (or matrices in the bipartite case), it has Lebesgue measure zero; this follows from the fact that any set defined by (non-trivial) polynomial equations has zero Lebesgue measure. A good metaphor for this situation is depicted in Figure 6.1.

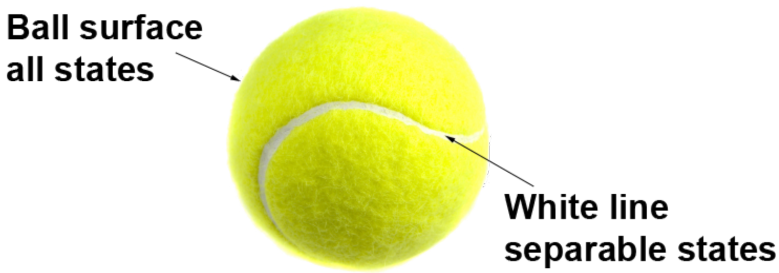


Figure 6.1: The surface of a tennis ball represents the set of pure quantum states, while the solid ball (its convex hull) represents the set of mixed states. The white rubber curve on the surface represents pure separable states. Its convex hull, a complicated objects represents mixed separable states.

Proposition 6.1.2. *Let* $|\varphi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ *be a random pure quantum state. If* $d_{1,2} \geq 2$,

$$\mathbb{P}\left[\,|\varphi\rangle \text{ is entangled}\right] = 1. \tag{6.1}$$

6.2 Generating random pure states

Although random pure quantum states are defined via the Lebesgue measure on the unit sphere of the complex Hilbert space corresponding to the quantum system in question, the easiest way to sample them and to analyze their properties is via the Gaussian distribution.

The Gaussian (or normal) distribution is arguably the most important probability distribution in mathematics and in science, due to the *Central Limit Theorem*: properly normalized sums of independent, identically distributed (i.i.d.) random variables converge to a Gaussian distribution.

In the real case, a *Gaussian distribution* of mean m and variance σ^2 has the following density with respect to the Lebesgue measure $\mathrm{d}x$:

$$\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-m^2)}{2\sigma^2}\right); \tag{6.2}$$

if X is such a random variable, we write $X \sim \mathcal{N}(m, \sigma^2)$, see Figure 6.2, left panel, for some examples. One can consider multi-dimensional Gaussian distributions, characterized by a vector $m \in \mathbb{R}^d$ and a positive definite *covariance matrix* $\Sigma \in \mathcal{M}_d^+(\mathbb{R})$. The density of such a random vector $\mathbb{R}^n d \ni X \sim \mathcal{N}(m, \Sigma)$ reads

$$\frac{1}{\sqrt{(2\pi)^d \det \Sigma}} \exp\left(-\frac{1}{2}\langle x-m, \Sigma^{-1}(x-m)\rangle\right). \tag{6.3}$$

Of importance in what follows is the multi-variate *standard* (i.e. zero mean, identity variance) complex case, where a random variable $Z \in \mathbb{C}^d$ is said to have a standard normal distribution if it has density

$$\frac{1}{\pi^d} \exp(-\|z\|^2/2). \tag{6.4}$$

In particular, a scalar standard complex random variable Z has independent real and imaginary parts, both having distribution $\mathcal{N}(0, 1/2)$, see Figure 6.2, right panel. More general complex Gaussian vectors $Z \in \mathbb{C}^d$ are described by a complex vector m and a positive definite complex covariance matrix Σ:

$$\forall i, \qquad \mathbb{E}Z_i = m_i \tag{6.5}$$

$$\forall i,j, \qquad \mathbb{E}[\bar{Z}_i Z_j] = \Sigma_{ij}. \tag{6.6}$$

The Gaussian distribution has the following important property: it is invariant with respect to the unitary group: if $Z \in \mathbb{C}^d$ is a complex Gaussian random vector, then, for any unitary operator $U \in \mathcal{U}_d$, the random variable UZ has also a complex standard Gaussian distribution. This, together with the fact that the Lebesgue (uniform) measure on the unit sphere is the unique probability measure on the sphere of a Hilbert space invariant with respect to all unitary rotations yields the following result.

Proposition 6.2.1. *Let $g \in \mathbb{C}^d$ be a standard complex Gaussian vector. Then, the normalized vector*

$$|\psi\rangle := \frac{g}{\|g\|} \tag{6.7}$$

is a random uniform pure quantum state. Moreover, the random variables $|\psi\rangle$ and $\|g\|$ are independent.

Note that the random variable $2\|g\|^2$ has a χ^2 distribution with $2d$ degrees of freedom. In particular, it has moments

$$\mathbb{E}\|g\|^{2p} = d(d+1)\cdots(d+p-1). \tag{6.8}$$

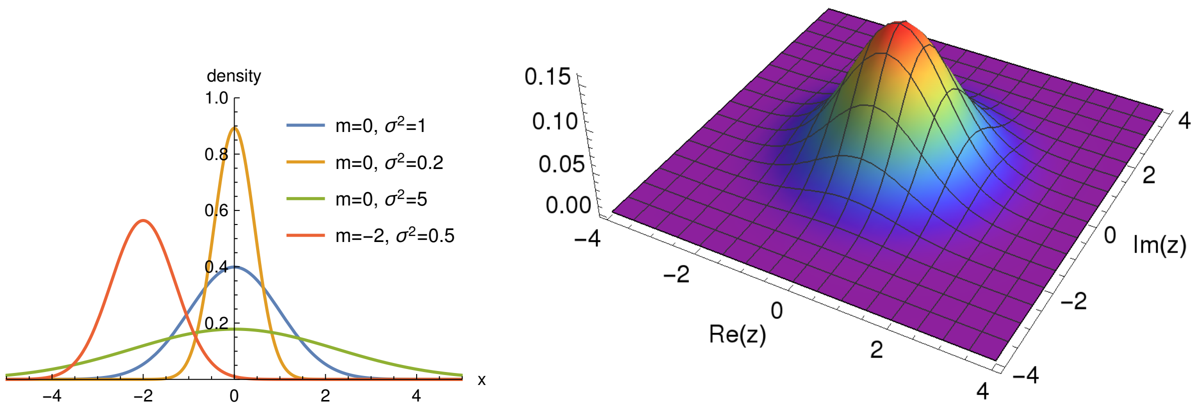


Figure 6.2: Gaussian distributions, in the real case (left) and in the complex case (right).

This result provides a very convenient method to sample random pure states on a computer: sample a standard complex Gaussian vector (using $2d$ independent real standard Gaussians):

$$z = \frac{1}{\sqrt{d}} \left(\sum_{k=1}^{d} x_k + \mathrm{i} y_k \right) \tag{6.9}$$

and normalize it.

6.3 Graphical Wick integration

We now address the question of computing integrals with respect to a Gaussian distribution. The combinatorial method described below is known in the literature as *Wick's formula*, or Isserlis' formula [Iss18]. We denote below by $P_2(k)$ the set of pair-partitions of the set $[k] = \{1, 2, \ldots, k\}$; for example,

$$P_2(4) = \{\, \{\{1,2\},\{3,4\}\}\, , \, \{\{1,3\},\{2,4\}\}\, , \, \{\{1,4\},\{2,3\}\}\, \} = \{ \quad , \quad , \quad \}.$$

Theorem 6.3.1. *Let Z be a (complex) Gaussian n-variate random vector with zero mean. Then, for all $i_1, i_2, \ldots, i_k \in [n]$, we have*

$$\mathbb{E}[Z_{i_1} Z_{i_2} \cdots Z_{i_k}] = \sum_{\pi \in P_2(k)} \prod_{\{s,t\} \in \pi} \mathbb{E}[Z_{i_s} Z_{i_t}]. \tag{6.10}$$

Proof. We shal prove the statement in the real case and leave the complex setting to the reader. First, note that if k is odd, both sides are zero: the LHS is zero by the invariance of a centered Gaussian distribution over a global sign change, while the RHS is zero since there are no pair partitions of $[k]$; we assume thus $k = 2r$. The proof strategy follows [Wit85]. The first ingredient of the proof is a *Laplace transform*: for all $\lambda \in \mathbb{R}^n$, we have

$$\mathbb{E} \exp\langle \lambda, Z \rangle = \exp\left(\frac{\langle \lambda, \Sigma\lambda \rangle}{2} \right). \tag{6.11}$$

We leave the proof of the claim above as an exercise, it follows from a linear change of variables in the Gaussian integral. Taking partial derivatives with respect to the λ_{i_s} variables and evaluating at $\lambda = 0$, we obtain

$$\mathbb{E}[Z_{i_1} Z_{i_2} \cdots Z_{i_k}] = \left. \frac{\partial^k}{\partial \lambda_{i_1} \cdots \partial \lambda_{i_k}} \right|_{\lambda=0} \exp\left(\frac{\langle \lambda, \Sigma \lambda \rangle}{2} \right). \tag{6.12}$$

To evaluate the derivative on the RHS, we use *Faà di Bruno's formula for the chain rule*, see [Har06, Proposition 1 and equation (4)]:

$$\frac{\partial^k}{\partial x_1 \cdots \partial x_k} f(y) = \sum_{\pi \in P(k)} f^{(\#\pi)}(y) \prod_{B \in \pi} \frac{\partial^{|B|} y}{\prod_{j \in B} \partial x_j}, \tag{6.13}$$

where the sum is over *all* partitions π of $[k]$, and $\#\pi$ denotes the number of blocks of a given partition π. In our situation, f above is the exponential function, so $f^{(\#\pi)} = f = \exp$, while y is a quadratic function of the x variables, so only *pair partitions* survive. □

It is a remarkable property of the Gaussian distribution that all the moments of the distribution can be computed using only the covariance. For example, for a centered Gaussian vector Z having covariance matrix Σ, we have

$$\mathbb{E}[Z_1 Z_2 Z_3 Z_4] = \Sigma_{12}\Sigma_{34} + \Sigma_{13}\Sigma_{24} + \Sigma_{14}\Sigma_{23}. \tag{6.14}$$

Since the number of pair partitions of $[2n]$ is

$$|P_2(2n)| = (2n-1)(2n-3)\cdots 5 \cdot 3 \cdot 1 =: (2n)!!, \tag{6.15}$$

we have the following corollary.

Corollary 6.3.2. *If X is a real standard Gaussian random variable, we have, for all $n \geq 0$:*

$$\mathbb{E}[X^{2n}] = (2n)!! \tag{6.16}$$
$$\mathbb{E}[X^{2n+1}] = 0. \tag{6.17}$$

For Z a complex standard Gaussian, he have

$$\mathbb{E}[\bar{Z}^m Z^n] = \delta_{m,n}(m+n)!!. \tag{6.18}$$

We shall now recast the Wick formula above in the graphical formalism described previously. Consider a diagram which contains a new special box G corresponding to a *Gaussian random matrix* (i.e. the entries of the matrix are i.i.d. standard complex Gaussian random variables). We shall compute the expected value of a random diagram with respect to the Gaussian probability measure; as we shall see, this operation will consist of *expanding* the diagram, by erasing the Gaussian boxes and replacing them with wires.

To start, consider $\mathcal{D}$ a diagram which contains, amongst other constant tensors, boxes corresponding to independent Gaussian random matrices of *covariance one* (identity). One can deal with more general Gaussian matrices by multiplying the standard ones with constant matrices. Note that a box can appear several times, adjoints of boxes are allowed and the diagram may be disconnected. Also, Gaussian matrices need not be square.

The expectation value of such a random diagram $\mathcal{D}$ can be computed by a *removal* procedure. Without loss of generality, we assume that we do not have in our diagram adjoints of Gaussian matrices, but instead their complex conjugate box. This assumption allows for a more straightforward use of the Wick formula from Theorem 6.3.1. We can assume that $\mathcal{D}$ contains only one type of random Gaussian box G; other independent random Gaussian matrices are assumed constant at this stage as they can be removed in the same manner afterwards.

A removal of the diagram $\mathcal{D}$ is a pairing between *Gaussian boxes* G and their conjugates $\bar{G}$. The set of removals is denoted by $\mathrm{Rem}_G(\mathcal{D})$ and it may be empty: if the number of G boxes is different from the number of $\bar{G}$ boxes, then $\mathrm{Rem}_G(\mathcal{D}) = \emptyset$ (since no pairing between matrices and their conjugates can exist). Otherwise, a removal r can identified with a permutation $\alpha \in \mathcal{S}_p$, where p is the number of G and $\bar{G}$ boxes. In the Gaussian/Wick calculus, one pairs conjugate boxes: white and black decorations are paired in an identical manner, hence only one permutation is needed to encode the removal.

To each removal r associated to a permutation $\alpha \in \mathcal{S}_p$ corresponds a removed diagram $\mathcal{D}_r$ constructed as follows. One starts by erasing the boxes G and $\bar{G}$, but keeps the decorations attached to these boxes. Then, the decorations (white *and* black) of the i-th G box are paired with the decorations of the $\alpha(i)$-th $\bar{G}$ box in a coherent manner, see Figure 6.3.

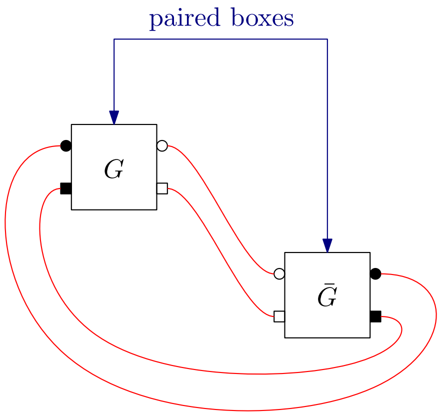


Figure 6.3: Pairing of boxes in the Gaussian case

The graphical reformulation of the Wick formula from Theorem 6.3.1 becomes the following theorem, which we state without proof.

Theorem 6.3.3. *The following holds true:*

$$\mathbb{E}_G[\mathcal{D}] = \sum_{r \in \mathrm{Rem}_G(\mathcal{D})} \mathcal{D}_r. \tag{6.19}$$

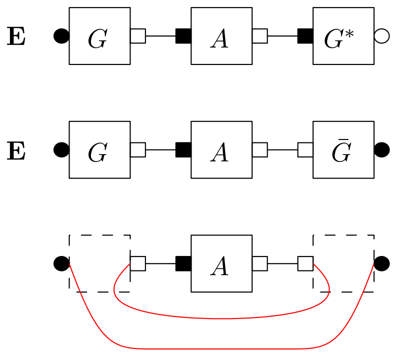
In Figure 6.4, we present an example of application of the theorem above. We consider, on the first row, the diagram corresponding to $\mathbb{E}[GAG^*]$, where $G \in \mathcal{M}_{n\times k}(\mathbb{C})$ is a $n \times k$ Gaussian matrix, and $A \in \mathcal{M}_k(\mathbb{C})$ is a square, deterministic matrix. The first row contains the diagram $\mathcal{D}$ associated to the algebraic expression. In the second row, we rewrite the same diagram, replacing G^* by $\bar{G}^\top$, in order to be able to apply Theorem 6.3.3. The third row contains the result of the application: we erase the $G/\bar{G}$ boxed and we add the wires corresponding to the permutation $(1) \in \mathcal{S}_1$ (in red). We recognize the diagrams for the identity matrix and for the trace of A: $\mathbb{E}[GAG^*] = \mathrm{Tr}(A)I_n$.

6.4 Two examples

In this section we shall use the graphical Wick formula introduced in the previous section to compute two important examples.

For the first, easier case, let us consider

$$F_1 := \int_{\|x\|=1} |x\rangle\langle x| \, \mathrm{d}\sigma(x) \tag{6.20}$$



$\mathrm{Tr}(A) \cdot I_n$

Figure 6.4: Applying Theorem 6.3.3 to compute $\mathbb{E}[GAG^*]$.

where σ is the Lebesgue measure on the unit sphere of $\mathbb{C}^d$. Using Proposition 6.2.1 and eq. (6.8), we relate our problem to a Gaussian integral:

$$d \cdot F_1 = \int_{g \text{ Gaussian}} |g\rangle\langle g| = \mathbb{E}gg^*. \tag{6.21}$$

Using the Gaussian Wick formula, we have $\mathbb{E}gg^* = I_d$ (see Figure 6.5), and thus $F_1 = I/d$: the average value of a random pure state is the maximally mixed state.

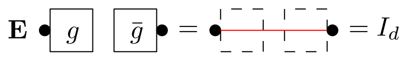


Figure 6.5: The average of gg^*, where g is a standard complex Gaussian vector.

Let us now move to the second example, the one used in the proof of Proposition 5.1.4:

$$F_2 := \int_{\|x\|=1} |x\rangle\langle x| \otimes |\bar{x}\rangle\langle \bar{x}| \, \mathrm{d}\sigma(x) \tag{6.22}$$

As before, we can relate it to a Gaussian integral, as follows:

$$F_2 = \frac{\mathbb{E}gg^* \otimes \bar{g}\bar{g}^*}{d(d+1)}. \tag{6.23}$$

Using the graphical Wick formula to evaluate the Gaussian integral (see Figure 6.6), we have

$$F_2 = \frac{d\omega_d + I_{d^2}}{d(d+1)} = \frac{1}{d+1}\omega_d + \left(1 - \frac{1}{d+1}\right)\frac{I}{d^2}. \tag{6.24}$$

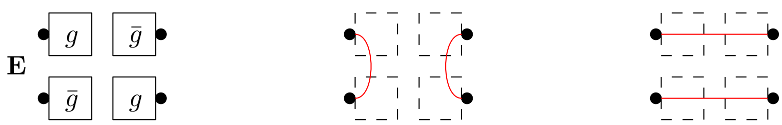


Figure 6.6: A Gaussian integral (left) and its two resulting diagrams (center and right).

6.5 Mixed states

The probability of entanglement for mixed states is a much more subtle question. To begin with, we can infer from Theorem 3.2.4 that any probability measure which has positive density with respect to the Lebesgue measure on the set of density matrix must assign a non-zero probability to the set of separable states.

The first thing we need to do is to endow the set of density matrices with a probability measure. Contrary to the case of pure states, there is no unique candidate for a probability measure on the convex body $\mathcal{M}_d^{1,+}$. Of course, the set of states inherits the Lebesgue measure of its ambient space, and one can normalize it to have unit mass. We shall see however that the Lebesgue measure is just a special case of a one parameter family of probability distributions which are very natural, both from a mathematical and from a physical viewpoint. Before going into details, let us briefly mention here another distribution on the set of states which has received a lot of attention, and which is motivated by considerations from statistics, the *Bures measure* [Hal98, SZ03, OSŻ10].

Let us introduced the family of *induced measures* starting from a physical perspective. Assume that the system of interest (modelled by the Hilbert space $\mathbb{C}^d$) is coupled to a s-dimensionnal environment $\mathbb{C}^s$ and that the joint system is in a pure state $|\psi\rangle$, which is distributed uniformly on the unit sphere of the product Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^s \cong \mathbb{C}^{ds}$. The reduced density matrix $\rho = \mathrm{Tr}_s |\psi\rangle\langle\psi|$ is a random mixed quantum state, and the *induced measure of parameters* d, s is the distribution of this random matrix. Note that ρ is a $d \times d$ random matrix, the parameter s appearing in the expression of its denisty. One can compute the probability distribution of this random matrix [ŻS01, ŻPNC11]

$$\mathrm{d}\mathbb{P}(\rho) = C_{d,s} \det \rho^{s-d} \mathbf{1}_{\rho \geq 0,\, \mathrm{Tr}\,\rho = 1} \mathrm{dLeb}(\rho), \tag{6.25}$$

where $C_{d,s}$ is a normalizing constant and Leb is the Lebesgue measure on the set of $d \times d$ hermitian matrices. In particular, it is a remarkable fact [ŻS03] that, for $s = d$ (i.e. the size of the envoronment is equal to the size of the system of interest), one recovers a uniform density, thus the Lebesgue measure (or the Hilbert-Schmidt measure) on the set of density matrices. Integrating out the Haar-distributed eigenvectors from (6.25), one obtains the probability density of the spectrum $(\lambda_1, \ldots, \lambda_d)$ of ρ, with respect to the Lebesgue measure on the probability simplex $\Delta_{d-1} := \{x \in \mathbb{R}^d : x_i \geq 0 \text{ and } \sum_i x_i = 1\}$:

$$\mathrm{d}\mathbb{P}(\lambda_1, \ldots, \lambda_d) = C'_{d,s} \prod_{i=1}^{d} \lambda_i^{s-d} \prod_{1 \leq i < j \leq d} (\lambda_i - \lambda_j)^2 \mathbf{1}_{\lambda_i \geq 0,\, \sum_i \lambda_i = 1} \mathrm{dLeb}(\lambda), \tag{6.26}$$

6.6 Wishart matrices

Historically the first ensemble of random matrices having been studied is the Wishart ensemble [Wis28], see [BS10, Chapter 3] or [AGZ10, Section 2.1] for a modern presentation.

Definition 6.6.1. *Let $G \in \mathcal{M}_{d \times s}(\mathbb{C})$ be a random matrix with complex, standard, i.i.d. Gaussian entries. The distribution of the positive-semidefinite matrix $W = GG^* \in \mathcal{M}_d(\mathbb{C})$ is called a* Wishart distribution *of parameters (d, s) and is denoted by $\mathcal{W}_{d,s}$.*

The study of the asymptotic behavior of Wishart random matrices is due to Marčenko and Pastur [MP67], while the stronger convergence results have been proved by analytic tools such as determinantal point processes; one can also recover the stronger forms of the theorem as direct consequences of the much more general results [Mal12]. Since we aim at giving complete proofs of our results, we state it here in a rather week form: the convergence in moments.

Definition 6.6.2. *A sequence of random matrices X_d is said to* converge in moments *to a probability distribution ν if for all positive integers p, we have*

$$\lim_{d \to \infty} \mathbb{E} \int t^p \mathrm{d}\mu_{X_d} = \mathbb{E} \frac{1}{d} \mathrm{Tr}(X_d^p) = \int t^p \mathrm{d}\nu, \tag{6.27}$$

where μ_{X_d} *is the* empirical eigenvalue distribution *of* X_d

$$\mu_{X_d} = \frac{1}{d}\sum_{i=1}^{d} \delta_{\lambda_i(X_d)}. \tag{6.28}$$

Theorem 6.6.3. *Consider a sequence* s_d *of positive integers which behaves as* $s_d \sim cd$ *as* $d \to \infty$*, for some constant* $c \in (0, \infty)$*. Let* W_d *be a sequence of positive-semidefinite random matrices such that* W_d *is distributed according to* $\mathcal{W}_{d,s_d}$*. Then, the sequence* W_d *converges in moments to the* Marčenko-Pastur distribution π_c *given by*

$$\pi_c = \max(1-c, 0)\delta_0 + \frac{\sqrt{(b-x)(x-a)}}{2\pi x}\,\mathbf{1}_{(a,b)}(x)\,\mathrm{d}x, \tag{6.29}$$

where $a = (1-\sqrt{c})^2$ *and* $b = (1+\sqrt{c})^2$.

The Marčenko-Pastur distribution π_c is sometimes called the *free Poisson distribution*, see [NS06, Proposition 12.11]. We plotted in Figure 6.7 its density in the cases $c = 1$ and $c = 4$.

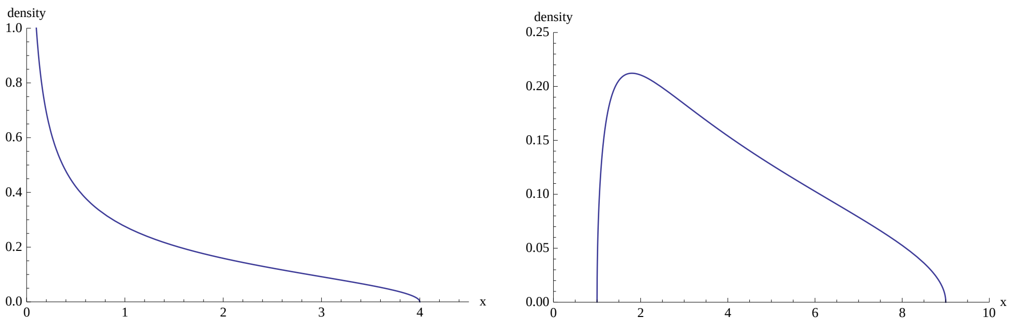


Figure 6.7: The density of the Marčenko-Pastur distributions π_1 (left) and π_4 (right).

Remark 6.6.4. *The Dirac mass appearing in* (6.29) *is due to the fact that if* $c < 1$*, the matrix* W_d *is rank deficient. Since* $cd < d$*, a fraction* $1 - c$ *of the eigenvalues of* W_d *are null, yielding the Dirac mass at zero.*

it is a remarkable fact that random quantum states following the induced distribution of parameters (d, s) can also be obtained as normalized Wishart matrix of the same parameters, see also [Nec07, ŻPNC11]

$$\rho = \frac{W}{\operatorname{Tr} W} = \frac{GG^*}{\operatorname{Tr}(GG^*)}, \tag{6.30}$$

where G is a $d \times s$ random matrix with i.i.d. standard complex Gaussian entries. To establish this equivalence, one uses the independence of the random variables ρ and $\operatorname{Tr} W$ appearing above, see [Nec07, Proposition 4 and Corollary 1].

Chapter 7

Symmetric extensions

We shall discuss in this chapter quantum mixed states which are entangled, although they pass the PPT criterion; in other words, states ρ such that

$$\rho \in \mathcal{PPT}(d_1 : d_2) \setminus \mathcal{SEP}(d_1 : d_2) \tag{7.1}$$

We shall first construct such states, and then discuss the *extendibility hierarchy* [DPS04] of entanglement criteria, based on the quantum de Finetti theorem.

7.1 An example of a PPT entangled state

We shall construct in this section a mixed bipartite quantum state which is entangled and PPT. The construction is based on the following notion, introduced in [BDM+99].

Definition 7.1.1. *An* unextendible product basis *(UPB) of $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is a family of vectors $\{x_1, \ldots, x_k\} \subseteq \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ with the following three properties:*

- *it is orthonormal: $\forall 1 \leq i, j \leq k$, $\langle x_i, x_j \rangle = \delta_{ij}$*
- *it is product: $\forall 1 \leq i \leq k$, $x_i = a_i \otimes b_i$ for unit vectors $a_i \in \mathbb{C}^{d_1}$, $b_i \in \mathbb{C}^{d_2}$*
- *it cannot be extended by a product vector: there are no unit vectors $\alpha \in \mathbb{C}^{d_1}$ and $\beta \in \mathbb{C}^{d_2}$ such that $\langle x_i, \alpha \otimes \beta \rangle = 0$ for all $1 \leq i \leq k$.*

As a first example, note that the canonical basis $\{x_{i,j} = e_i \otimes f_j\}$, where e_i (resp. b_j) are bases of $\mathbb{C}^{d_1}$ (resp. $\mathbb{C}^{d_2}$), is an UPB. However, we consider such cases as trivial, and we shall be interested in incomplete UPBs, for which the third condition in Definition 7.1.1 is non-trivially satisfied.

Let us now consider the following example of two qutrits from [BDM+99]:

$$x_1 = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle) \tag{7.2}$$

$$x_2 = \frac{1}{\sqrt{2}}|2\rangle \otimes (|1\rangle - |2\rangle) \tag{7.3}$$

$$x_3 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle \tag{7.4}$$

$$x_4 = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle \tag{7.5}$$

$$x_5 = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle) \otimes (|0\rangle + |1\rangle + |2\rangle). \tag{7.6}$$

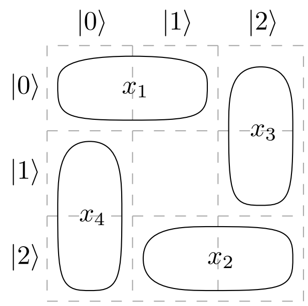


Figure 7.1: The "tiles" corresponding to the first four elements of the UPB from [BDM+99].

This construction is motivated by the "interlocking tiles" state from [BDF+99], see Figure 7.1 for a graphical representation of the first four states in the UPB. The fact that these elements form an orthonormal set is easily checked by hand.

Let us now show that there is no unit product state $\alpha \otimes \beta$ orthogonal to $x_1, \ldots, x_5$. Suppose there were such α, β. Then α must be orthogonal to at least three of

$$|0\rangle, |2\rangle, |0\rangle - |1\rangle, |1\rangle - |2\rangle, |0\rangle + |1\rangle + |2\rangle \tag{7.7}$$

or β must be orthogonal to at least three among the above. Since any three vectors among the five above are linearly independent, a contradiction ensues, proving the claim.

Let us now show that any (non-trivial) UPB can be used to construct mixed states which are entangled and PPT.

Proposition 7.1.2. *Let $X := \{x_1, \ldots, x_k\} \subseteq \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ be a non-trivial (i.e. $k < d_1 d_2$) UPB. Then, the quantum state*

$$\rho_X := \frac{1}{d_1 d_2 - k} \left(I_{d_1 d_2} - \sum_{i=1}^{k} |x_i\rangle\langle x_i| \right) \tag{7.8}$$

is PPT entangled.

Proof. First, note that X being an orthonormal family implies that ρ_X is positive semidefinite, and the normalization is chosen such that it has unit trace. The same arguments apply for it's partial transpose

$$\rho_X^\Gamma = \frac{1}{d_1 d_2 - k} \left(I_{d_1 d_2} - \sum_{i=1}^{k} |a_i \otimes b_i\rangle\langle a_i \otimes b_i| \right)^\Gamma = \frac{1}{d_1 d_2 - k} \left(I_{d_1 d_2} - \sum_{i=1}^{k} |a_i \otimes \bar{b}_i\rangle\langle a_i \otimes \bar{b}_i| \right) \tag{7.9}$$

where we have written $x_i = a_i \otimes b_i$, and that $y_i := a_i \otimes \bar{b}_i$ form another UPB. Hence, $\rho_X^\Gamma \geq 0$, i.e. ρ_X is PPT.

Let us now show that ρ_X is entangled. Suppose that ρ_X were separable, and consider a separable decomposition

$$\rho_X = \sum_{j=1}^{r} |z_j\rangle\langle z_j| \tag{7.10}$$

for product states $z_1, \ldots, z_r$. Note however that ρ_X was constructed to be the (normalized) projection on the space $\mathcal{X}^\perp$, where $\mathcal{X} := \operatorname{span} X$. This implies that the product vectors z_j are orthogonal to all the elements in X, contradicting the non-extendibility of the UPB X. □

The construction of PPT entangled states using UPBs is just one of the many possible ways to produce such states. For example, in the case of qubit-qudit systems ($d_1 = 2$, $d_2 \geq 4$), the

UPB method cannot work, but PPT entangled states exist. The following is a generalization of [Hor97, Section 4.2], see also [KVSW09, Example 2.15] and to [KW93, Proposition 3.1].

$$\rho = \begin{bmatrix} I & B^* \\ B & C \end{bmatrix}, \tag{7.11}$$

with $n \times n$ matrices

$$B = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} \frac{1}{2}(x+1) & 0 & 0 & \cdots & 0 & 0 & \frac{1}{2}\sqrt{x^2-1} \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ \frac{1}{2}\sqrt{x^2-1} & 0 & 0 & \cdots & 0 & 0 & \frac{1}{2}(x+1) \end{bmatrix}.$$

Proposition 7.1.3. *Assume $n \geq 2$ and $x \geq 1$. The PPT matrix ρ in (7.11) is separable iff. $n = 2, 3$ or $x = 1$. Hence, for $n \geq 4$ and $x > 1$, ρ is PPT entangled.*

7.2 The DPS extendibility hierarchy

We shall describe here a *hierarchy of criteria* [DPS04] with the important property that, when considering them together, they characterize exactly separability.

The starting point is the following observation. Consider a separable state $\rho \in \mathcal{SEP}(d_1 : d_2)$ with a separable decomposition

$$\rho_{AB} = \sum_{i=1}^{r} |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i| \tag{7.12}$$

and define, for $k \geq 1$, it's k-extension by

$$\rho_{AB_1B_2\cdots B_k} = \sum_{i=1}^{r} |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|^{\otimes k}. \tag{7.13}$$

Note that the notion of extendibility discussed in this section has nothing to do with the unextendible product bases from Definition 7.1.1.

7.3 The quantum de Finetti theorem

We prove in this section a fundamental result in quantum theory, the quantum de Finetti theorem. This result makes precise the following intuitive fact: in a permutation-symmetric quantum state, "small marginals" should not be "very" entangled.

This fact is closely related to a different fundamental concept in quantum information theory, that of *monogamy of entanglement*. Consider a three-partite quantum state ρ_{ABC} such that Alice and Bob are maximally entangled:

$$\rho_{AB} = \operatorname{Tr}_C \rho_{ABC} = \omega. \tag{7.14}$$

Then, since ρ_{AB} is pure, it follows from Proposition 3.2.3 that Charlie cannot be entangled with either Alice or Bob (in other words, entanglement is monogamous, see Figure 7.2):

$$\rho_{ABC} = \rho_{AB} \otimes \rho_C \quad \Longrightarrow \quad \rho_{AC} = \rho_A \otimes \rho_C \quad \text{and} \quad \rho_{BC} = \rho_B \otimes \rho_C. \tag{7.15}$$

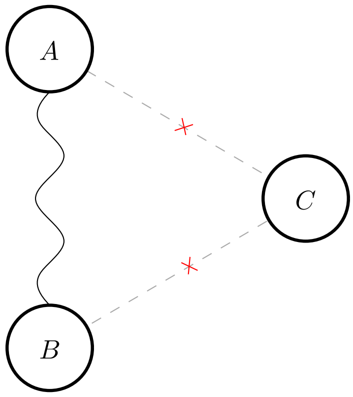


Figure 7.2: Monogamy of entanglement: if Alice and Bob are maximally entangled, Charlie cannot be entangled with either of them.

Another, more physical, point of view on quantum de Finetti theorem comes from mean-field theory, and was at the origin of this type of results [RW89, Rou15]. Consider a mean-field Hamiltonian on n quantum systems (n should be large here):

$$H = \sum_{\text{all } \{i,j\}} h_{ij}, \tag{7.16}$$

where $h_{ij} = h_{ij}^* \in \mathcal{M}_{d^2}(\mathbb{C})$ is a 2-particle interaction term. Assuming the ground state $|\psi\rangle$ of this n-body system is non-degenerate, it should be permutation invariant, that is

$$|\psi\rangle \in \vee^n(\mathbb{C}^d) \tag{7.17}$$

where $\vee^n(\mathbb{C}^d) \subseteq (\mathbb{C}^d)^{\otimes n}$ is the symmetric subspace of the n-particle tensor product. The quantum de Finetti theorem makes precise the following fact: for a (relatively) small number of particles $k \ll n$, we have

$$\rho_{1\cdots k} = \mathrm{Tr}_{(k+1)\cdots n}\, |\psi\rangle\langle\psi| \approx \int_{x\in\mathbb{C}^d,\, \|x\|=1} p_x |x\rangle\langle x|\, \mathrm{d}\sigma(x) \in \mathcal{SEP}(\underbrace{d : d : \cdots : d}_{k \text{ times}}). \tag{7.18}$$

Before stating and proving the quantum de Finetti theorem, let us review some basic facts about the symmetric subspace, the fundamental mathematical object underlying the results in this section; we refer to the excellent [Har13] for more details.

A tensor $x = (x_{i_1,i_2,\ldots,i_n}) \in (\mathbb{C}^d)^{\otimes n}$ is called *symmetric* if its coefficients are invariant by permutation of indices:

$$\forall \pi \in \mathcal{S}_n, \qquad x_{i_1,i_2,\ldots,i_n} = x_{i_{\pi(1)},i_{\pi(2)},\ldots,i_{\pi(n)}}. \tag{7.19}$$

For example, tensor products $a^{\otimes n}$ are symmetric, but there exist symmetric tensors which are not of this form, for example (see Chapter 8): $|000\rangle + |111\rangle \in (\mathbb{C}^2)^{\otimes 3}$. Actually, we have

$$\vee^n(\mathbb{C}^d) \subseteq (\mathbb{C}^d)^{\otimes n} = \mathrm{span}\{a^{\otimes n} \,:\, a \in \mathbb{C}^d\}. \tag{7.20}$$

Theorem 7.3.1. *Let $1 \le k \le n$ and $d \ge 1$. For any symmetric quantum state $|\psi\rangle \in \vee^n(\mathbb{C}^d)$, there exists a probability measure μ on the unit sphere of $\mathbb{C}^d$ such that*

$$\left\| \mathrm{Tr}_{n-k}\, |\psi\rangle\langle\psi| - \int_{\|x\|=1} |x\rangle\langle x|^{\otimes k}\, \mathrm{d}\mu(x) \right\|_1 \le * * *. \tag{7.21}$$

Chapter 8

Multipartite entanglement

In this chapter, we shall discuss the entanglement of *pure* multipartite quantum states. The corresponding problem for multipartite mixed states is of considerable difficulty, and not much is known about it [HHHH09, Section VII].

As in the bipartite case, pure states of quantum systems are mathematically represented by vectors in a tensor product space. Here, we shall consider m-partite quantum states, where the respective dimensions of the Hilbert space tensor factors are, respectively, $d_1, d_2, \ldots, d_m$.

Example 8.0.1. *The most famous 3-qubit states are the* GHZ state *[GHZ89]*

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{8.1}$$

and the W state *[DVC00]*

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle). \tag{8.2}$$

One can easily create in Quirk

1. *A GHZ state*
2. *A W state*

In the multipartite setting, separability and entanglement are defined in a similar way, using product tensors.

Definition 8.0.2. *A multipartite pure quantum state $|\varphi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_m}$ is called separable if it can be written as a product tensor*

$$|\varphi\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots |x_m\rangle. \tag{8.3}$$

A non-separable quantum state is called entangled.

Testing whether a multipartite quantum state is separable is also efficient.

Lemma 8.0.3. *A pure quantum state $|\varphi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_m}$ is separable iff $|\varphi\rangle$ is bi-separable with respect to the following bi-partitions*

$$\begin{gathered}\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2 \cdots d_m} \\ \mathbb{C}^{d_1 d_2} \otimes \mathbb{C}^{d_3 \cdots d_m} \\ \vdots \\ \mathbb{C}^{d_1 \cdots d_{m-1}} \otimes \mathbb{C}^{d_m}.\end{gathered} \tag{8.4}$$

Proof. Let us prove the result in the tripartite case $m = 3$, the general case being similar. From the first condition, we obtain a decomposition

$$|\varphi\rangle = |\alpha\rangle \otimes |\psi\rangle_{BC}, \tag{8.5}$$

while from the second condition we have

$$|\varphi\rangle = |\psi\rangle_{AB} \otimes |\gamma\rangle. \tag{8.6}$$

Taking the partial trace over A of the latter equation and plugging the result in the former, we have

$$|\varphi\rangle\langle\varphi| = |\alpha\rangle\langle\alpha| \otimes (\operatorname{Tr}_A |\psi\rangle\langle\psi|_{AB}) \otimes |\gamma\rangle\langle\gamma|, \tag{8.7}$$

proving that $|\varphi\rangle$ is separable. □

It is a remarkable fact that the GHZ and W states are differently entangled [DVC00], see the last section of this chapter for the details.

8.1 Tensor rank

We have seen that, for bipartite pure states, the *Schmidt rank* R of a quantum state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ plays a particular role with respect to separability: $|\psi\rangle$ is separable if and only if $R = 1$. The tensor rank is the natural generalization of this notion in the multipartite setting.

Definition 8.1.1. *The tensor rank of $x \in \mathbb{C}^{d_1} \otimes \cdots \mathbb{C}^{d_m}$ is the smallest integer $R(x)$ such that x can be written as a sum of $R(x)$ simple tensors:*

$$x = \sum_{i=1}^{R(x)} a_i^{(1)} \otimes a_i^{(2)} \otimes \cdots \otimes a_i^{(m)}. \tag{8.8}$$

The tensor rank reduces, in the bipartite case ($m = 2$) to the Schmidt rank for 2-tensors (resp. the usual matrix rank):

$$x = \sum_{i=1}^{r} a_i \otimes b_i \tag{8.9}$$

$$X = \sum_{i=1}^{r} |a_i\rangle\langle b_i|. \tag{8.10}$$

Note however that computing the tensor rank of a m-tensor is an NP-hard problem for $m \geq 3$ [Hås90, Theorem 1] or [HL13, Theorem 8.2]; this is an important difference with the bipartite case, where the computation of the rank can be done efficiently via the SVD.

Example 8.1.2. *The tensor rank of the GHZ state is $R(|\mathrm{GHZ}\rangle) = 2$. Indeed, the decomposition (8.1) shows that $R(|\mathrm{GHZ}\rangle) \leq 2$, while the fact that $|\mathrm{GHZ}\rangle$ is not separable (since its 1-marginal is the maximally mixed state) proves that $R(|\mathrm{GHZ}\rangle) \geq 2$.*

Proposition 8.1.3. *The rank of the W state is $R(|\mathrm{W}\rangle) = 3$.*

Proof. From the decomposition (8.2) we have $R(|\mathrm{W}\rangle) \leq 3$, while from the fact that the W state is entangled we have $R(|\mathrm{W}\rangle) \geq 2$. To prove the claim, we need to rule out a 2-term decomposition of $|\mathrm{W}\rangle$ as a sum of simple tensors. Assume there is a decomposition

$$|\mathrm{W}\rangle = a_1 \otimes b_1 \otimes c_1 + a_2 \otimes b_2 \otimes c_2 \tag{8.11}$$

where the two terms are not collinear (which cannot be the case since $|\mathrm{W}\rangle$ is not separable). This would imply that the range of the operator $\mathrm{Tr}_A |\mathrm{W}\rangle\langle\mathrm{W}|$ contains at least two non-collinear product operators: $b_1 \otimes c_1$ and $b_2 \otimes c_2$. But a simple calculation proves that there is just one product operator in

$$\mathrm{Ran}\,\mathrm{Tr}_A |\mathrm{W}\rangle\langle\mathrm{W}| = \mathbb{C}|00\rangle \oplus \mathbb{C}(|01\rangle + |10\rangle), \tag{8.12}$$

finishing the proof. □

An important property of the rank is it's behavior with respect to local operations. Local operations and classical communication (when dealing with pure states) are mathematically characterized by the tensor product of unitary operations

$$U = U_1 \otimes \cdots \otimes U_m, \qquad (U_1, \ldots, U_m) \in \mathcal{U}_{d_1} \times \cdots \times \mathcal{U}_{d_m} \tag{8.13}$$

One can also consider the larger class of *stochastic local operations and classical communication*: we ask that transformations only succeed with non-zero probability (assuming in the protocol, some quantum measurements are performed). Two states $|\psi\rangle, |\varphi\rangle$ are SLOCC-equivalent (i.e. either one can be transformed in the other by SLOCC) if there exist invertible operators $A_1, \ldots, A_m$ such that

$$|\psi\rangle = A_1 \otimes \cdots \otimes A_m |\varphi\rangle. \tag{8.14}$$

It is clear that the tensor rank is a SLOCC invariant. In particular, we see that the GHZ and W states are *not* SLOCC equivalent.

Let us end this section by describing a very interesting phenomenon, specific to tensors, which is not present in the matrix world: the set of tensors of rank smaller than some constant might not be closed! For 2-tensors, matrices with rank smaller or equal than r can be characterized as the intersection of algebraic manifolds, defined by minors of order $r+1$, making the set trivially closed. For 3 tensors, we have, surprisingly

$$|\mathrm{W}\rangle = \lim_{\varepsilon \to 0} \frac{(|0\rangle + \varepsilon|1\rangle)^{\otimes 3} - |000\rangle}{\varepsilon}, \tag{8.15}$$

showing that the W state (which has rank 3) can be written as a limit of rank 2 states. This fact is captured by the notion of *border rank*, which we shall not discuss here.

8.2 Classification of 3 qubit entanglement

We present in this section a fundamental result in quantum information theory, the classification of $2 \otimes 2 \otimes 2$ entanglement under SLOCC equivalence [DVC02].

Before we study the 3 qubit case, let us point out that in the (arbitrary dimension) bipartite case, the (Schmidt) rank is a complete invariant: two quantum states are SLOCC-equivalent if and only if they have the same Schmidt rank.

We turn now to the case of three qubits, where the following result was proven in [DVC02]. We would also like to point out that this result was known in the mathematical community since the work of Le Paige in 1881 [LP81], present also in [GKZ94, Chapter 14, Example 4.5]. We point out that larger systems have a much more complicated structure (e.g. for one qubit and two qutrits, there are 17 different SLOCC entangled classes, see [HLT12]).

Theorem 8.2.1. *There are six SLOCC equivalence classes on* $(\mathbb{C}^2)^{\otimes 3}$*:*

- *Separable states* $(A - B - C)$
- *Three classes corresponding to bi-separable states* $(A - BC)$*,* $(B - AC)$*,* $(C - AB)$
- *The class of the W state* (W)

- *The class of the GHZ state* (GHZ)

Proof. Let us denote by $|\varphi\rangle \in \mathbb{C}^8$ an arbitrary 3 qubit state. First, note that the ranks of the 1-particle marginals:

$$r_A := \operatorname{rank} \operatorname{Tr}_{BC} |\varphi\rangle\langle\varphi|, \qquad r_B := \operatorname{rank} \operatorname{Tr}_{AC} |\varphi\rangle\langle\varphi|, \qquad r_C := \operatorname{rank} \operatorname{Tr}_{AB} |\varphi\rangle\langle\varphi| \tag{8.16}$$

are SLOCC invariants. The integer vector $r := (r_A, r_B, r_C)$ allows to differentiate 4 of the six classes, corresponding to separable ($r = (1,1,1)$) and bi-separable (one of the coordinates of r is 1) states.

We now consider the case where $r = (2,2,2)$. Note first that, by the result on the tensor ranks of the GHZ and W states from the previous section, the two classes of (GHZ) and (W) are different. To conclude, we only need to show that their union covers the whole set of genuinely entangled 3 qubit quantum states.

□

Bibliography

[AGZ10] Greg W Anderson, Alice Guionnet, and Ofer Zeitouni. *An introduction to random matrices*. Cambridge University Press, 2010. 37

[ALP+19] Guillaume Aubrun, Ludovico Lami, Carlos Palazuelos, Stanisław J Szarek, and Andreas Winter. Universal gaps for XOR games from estimates on tensor norm ratios. *Comm. Math. Phys.*, 2019. 15

[ALPP19] Guillaume Aubrun, Ludovico Lami, Carlos Palazuelos, and Martin Plavala. Entangleability of cones. *arXiv preprint arXiv:1911.09663*, 2019. 15

[AS17] Guillaume Aubrun and Stanisław J. Szarek. *Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory*, volume 223. American Mathematical Soc., 2017. 18, 25

[BDF+99] Charles H Bennett, David P DiVincenzo, Christopher A Fuchs, Tal Mor, Eric Rains, Peter W Shor, John A Smolin, and William K Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070, 1999. 40

[BDM+99] Charles H Bennett, David P DiVincenzo, Tal Mor, Peter W Shor, John A Smolin, and Barbara M Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82(26):5385, 1999. 39, 40

[BS10] Zhidong Bai and Jack W Silverstein. *Spectral analysis of large dimensional random matrices*, volume 20. Springer, 2010. 37

[DPS04] Andrew C Doherty, Pablo A Parrilo, and Federico M Spedalieri. Complete family of separability criteria. *Physical Review A*, 69(2):022308, 2004. 39, 41

[DVC00] Wolfgang Dür, Guifre Vidal, and J Ignacio Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62(6):062314, 2000. 43, 44

[DVC02] W Dür, G Vidal, and J Ignacio Cirac. Optimal conversion of nonlocal unitary operations. *Physical review letters*, 89(5):057901, 2002. 45

[GB02] Leonid Gurvits and Howard Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Physical Review A*, 66(6):062311, 2002. 18

[GHZ89] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Going beyond bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989. 43

[GKZ94] I Gelfand, M Kapranov, and Andrey V Zelevinsky. *Discriminants, resultants and multidimensional determinants. Reprint of the 1994 edition. Modern Birkhäuser Classics*. Birkhäuser Boston, Inc., Boston, MA, 1994. 45

[Hal98] Michael JW Hall. Random quantum correlations and density operator distributions. *Physics Letters A*, 242(3):123–129, 1998. 37

[Har06] Michael Hardy. Combinatorics of partial derivatives. *the electronic journal of combinatorics*, 13(1):1, 2006. 34

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013. 42

[Hås90] Johan Håstad. Tensor rank is np-complete. *Journal of algorithms (Print)*, 11(4):644–654, 1990. 44

[HH99] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59(6):4206, 1999. 29

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, 1996. 25, 26

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009. 5, 43

[HL13] Christopher J Hillar and Lek-Heng Lim. Most tensor problems are np-hard. *Journal of the ACM (JACM)*, 60(6):45, 2013. 44

[HLT12] Frédéric Holweck, Jean-Gabriel Luque, and Jean-Yves Thibon. Geometric descriptions of entangled states by auxiliary varieties. *Journal of Mathematical Physics*, 53(10):102203, 2012. 45

[Hor97] Pawel Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232(5):333–339, 1997. 41

[Iss18] Leon Isserlis. On a formula for the product-moment coefficient of any order of a normal frequency distribution in any number of variables. *Biometrika*, 12(1/2):134–139, 1918. 33

[KVSW09] Dmitry S Kaliuzhnyi-Verbovetskyi, Ilya M Spitkovsky, and Hugo J Woerdeman. Matrices with normal defect one. *arXiv preprint arXiv:0903.0090*, 2009. 41

[KW93] David P Kimsey and Hugo J Woerdeman. Minimal normal and commuting completions. *Linear and Multilinear Algebra*, 36:59–68, 1993. 41

[Lam18] Ludovico Lami. Non-classical correlations in quantum mechanics and beyond. *PhD thesis. arXiv preprint arXiv:1803.02902*, 2018. 15

[LP81] C Le Paige. Sur la théorie des formes binaires à plusieurs séries de variables. *Bull. Acad. Roy. Sci. Belgique (3), bf*, 2:40–53, 1881. 45

[Mal12] Camille Male. The norm of polynomials in large random and deterministic matrices. *Probability Theory and Related Fields*, 154(3-4):477–532, 2012. 37

[MP67] Vladimir A Marčenko and Leonid Andreevich Pastur. Distribution of eigenvalues for some sets of random matrices. *Sbornik: Mathematics*, 1(4):457–483, 1967. 37

[Nec07] Ion Nechita. Asymptotics of random density matrices. *Annales Henri Poincaré*, 8(8):1521–1538, 2007. 38

[NS06] Alexandru Nica and Roland Speicher. *Lectures on the combinatorics of free probability*, volume 13. Cambridge University Press, 2006. 38

[OSŻ10] V Osipov, Hans-Juergen Sommers, and K Życzkowski. Random bures mixed states and the distribution of their purity. *Journal of Physics A: Mathematical and Theoretical*, 43(5):055302, 2010. 37

[Pau02] Vern Paulsen. *Completely bounded maps and operator algebras*, volume 78. Cambridge University Press, 2002. 21

[Per96] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413, 1996. 26

[Rou15] Nicolas Rougerie. De finetti theorems, mean-field limits and bose-einstein condensation. *arXiv preprint arXiv:1506.05263*, 2015. 42

[RW89] GA Raggio and RF Werner. Quantum statistical mechanics of general mean field systems. *Helv. Phys. Acta*, 62(8):980–1003, 1989. 42

[SZ03] Hans-Jürgen Sommers and Karol Zyczkowski. Bures volume of the set of mixed quantum states. *Journal of Physics A: Mathematical and General*, 36(39):10083, 2003. 37

[Wis28] John Wishart. The generalised product moment distribution in samples from a normal multivariate population. *Biometrika*, pages 32–52, 1928. 37

[Wit85] CS Withers. The moments of the multivariate normal. *Bulletin of the Australian Mathematical Society*, 32(1):103–107, 1985. 33

[Wor76] Stanisław Lech Woronowicz. Positive maps of low dimensional matrix algebras. *Reports on Mathematical Physics*, 10(2):165–183, 1976. 26

[ŻPNC11] Karol Życzkowski, Karol A Penson, Ion Nechita, and Benoit Collins. Generating random density matrices. *Journal of Mathematical Physics*, 52(6):062201, 2011. 37, 38

[ŻS01] Karol Życzkowski and Hans-Jürgen Sommers. Induced measures in the space of mixed quantum states. *Journal of Physics A: Mathematical and General*, 34(35):7111, 2001. 37

[ŻS03] Karol Życzkowski and Hans-Jürgen Sommers. Hilbert-schmidt volume of the set of mixed quantum states. *Journal of Physics A: Mathematical and General*, 36(39):10115, 2003. 37