Quantum Information
week 4

Until the end of the course

- Separability/entanglement for mixed states. Measures of entanglement. Entanglement criteria. Entanglement Witnesses. Non locality, Bell inequalities. Quantum cryptography (week 4)
- Quantum computing. Basic notions of Quantum Complexity. The Quantum circuit model: gates, evolutions and measurements. Quantum algorithms (week 5/6)
- Quantum Information revisited: a summary of important concepts review during this course. Open questions (week 6)

In this lectures

- We will review what is entanglement for pure states. Introduce the problem of separability/entanglement for mixed bipartite states.
- We will introduce the quantification of entanglement.
- We will provide entanglement criteria: partial transposition, majorization, cross-norm, covariance matrix and entanglement witnesses.

Recall: properties of the tensor product

1. Let $\mathbb{H} = \mathbb{H}_1 \otimes \mathbb{H}_2$. Then the dimension of $|\mathbb{H}| = |\mathbb{H}_1| \times |\mathbb{H}_2|$

2. Suppose $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle$, and let $\{|i_1\rangle\}_{i_1=1}^{d_1}$, $\{|i_2\rangle\}_{i_2=1}^{d_2}$ be orthonormal basis of $\mathbb{H}_1, \mathbb{H}_2$. Then $|\psi\rangle = \sum_{i_1=1}^{d_1} \sum_{i_2=1}^{d_2} \phi_{i_1}\chi_{i_2}|i_1\rangle \otimes |i_2\rangle$

3. Suppose $A : \mathbb{H}_1 \to \mathbb{H}_1, \quad B = \mathbb{H}_2 \to \mathbb{H}_2$. Then $C : \mathbb{H} \to \mathbb{H}, C = A \otimes B$ is given by $C = \sum_{i_1,j_1} \sum_{i_2,j_2} A_{j_1,i_1} B_{j_2,i_2} |j_1\rangle\langle i_1| \otimes |j_2\rangle\langle i_2|$

4. The tensor product space $\mathbb{H} = \mathbb{H}_1 \otimes \mathbb{H}_2$ inherits all the properties of its constituent parts (linearity, multiplicative & additive identity etc etc)

Entanglement: q. correlations

1. Entanglemet deals with a generic form of quanum correlations, and is linked to the tensorial structure of the Hilbert space.
2. Entanglement is a propertie of composite quantum systems. We shall consider from now on bipartite quantum states

$$|\psi\rangle_{AB} \in \mathbb{H}_A \otimes \mathbb{H}_B$$

traditionally denoted as Alice and Bob.

Definition. Product states: $|\psi\rangle_{AB}$, is a product state iff $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\varphi\rangle_B$ that is if the local states are also pure states. Otherwise it is entangled

Definition. Schmidt decompostion: Every bipartite pure state can be expressed in its Schmidt form: $|\Psi\rangle_{AB} = \sum_{i=1}^{M} \sqrt{\lambda_i}\,|e_i\rangle\,|f_i\rangle$ where $\{|e_i\rangle\}(\{|f_i\rangle\})$ are orthonormal basis of $\mathbb{H}_A(\mathbb{H}_B)$, $\lambda_i \in \mathbb{R}, \lambda_i \geq 0 \forall \{i\}$, and $\sum_{\mathrm{i}} \lambda_{\mathrm{i}} = 1$.

Reduced states of composite systems

Given a bipartite pure state $|\Psi\rangle_{AB}$, to find its Schmidt decompostion we should calculate the reduced density matrix of the subsystems. In the Schmidt basis, both reduced density matrices are diagonal (This is the singular value decomposition!)

$$|\psi\rangle_{AB} = \sum_{i=1}^{\min(d_1,d_2)} \sqrt{\lambda_i}\, |e_i, f_i\rangle$$

Since

$$\rho_A \equiv Tr_B(|\psi\rangle_{AB}\langle\psi|) = \sum_i^{d_1} \lambda_i |e_i\rangle\langle e_i|$$

$$\rho_B \equiv Tr_A(|\psi\rangle_{AB}\langle\psi|) = \sum_i^{d_2} \lambda_i |f_i\rangle\langle f_i|$$

Entanglement: q. correlations

- Entanglemet deals with a generic form of quanum correlations, and is linked to the tensorial structure of the Hilbert space.
- Entanglement is a propertie of composite quantum systems. We shall consider from now generically bipartite quantum states (Alice & Bob)

$$|\psi\rangle_{AB} \in \mathbb{H}_A \otimes \mathbb{H}_B$$

- Entanglemet is arguably the most genuine property of quantum physics as allows to perform tasks that otherwise are impossible.
- Entanglement is considered to be a resource for quantum information tasks. There are other resources as for instance coherence, locality, asymmetry, etc..

Example of the use of pure state entanglement: super-dense coding

Super-Dense Coding: Alice wants to send two bits of information (classical) to Bob with a single use of a channel. How? Sharing forhand a maximally entangled state

Alice has bit a=(0,1) and the bit b=(0,1) and as well as maximally entangled state of two qubits of the form:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

She uses the following protocol:

(1) if a=1 (b=1) apply a σ_z (σ_x) to the qubit A of the state $|\Phi^+\rangle_{AB}$. If a=b=0 do noting

(2) Send qubit A of $|\psi\rangle_{AB}$ to Bob

(3) Bob performs a CNOT gate $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Example of the use of pure state entanglement: superdense coding

(4) Bob performs a Hadamar gate on control target $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

(5) Bob measures on his qubits to extract the value of the 2 bits.

Let's do it:

(i) write the protocol as a quantum circuit (it is easy)

(ii) classical bits are used here a controled bits. Depending on their value Alice does one operation or another.

(iii) For instance if Alice wants to send (0,0), the protocol gives the following output

$$|\Phi^{+}\rangle_{AB} \Rightarrow_{P1} |\Phi^{+}\rangle_{AB} \Rightarrow_{P3} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \Rightarrow_{P4} |00\rangle$$

Entanglement in mixed states

Definition: A quantum state $\rho_{AB} \in \mathscr{B}(\mathbb{H}_A \otimes \mathbb{H}_B)$ is said to be separable if the bipartite state can be written as

$$\rho_{AB} = \sum_i p_i \, (\rho_i^A \otimes \rho_i^B) = \sum_i q_i \, (|e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|)$$

with $p_i \geq 0$ and $\sum \mathrm{p_i} = 1$, ($\mathrm{q_i} \geq 0$ and $\sum \mathrm{q_i} = 1$). In other words the state ρ_{AB} is separable iff it is a convex combination of product of projectors in local states.

Remarks: To be separable means that the state can be prepared using local operations and classical communication. Such operatos are called LOCC

Quantification of entanglement

- Entanglement permits to do tasks that cannot be done with classica states: superdense coding, teleportation, and many algorithms
- Entanglement is therefore a RESOURCE for quantum information. Free states are separable states and LOCC are free operatins.
- Unit of entanglement is the e-bit, that is, the entanglement contained in a maximally entangled bipartite state of two-qubits
- What is the entanglement in an arbitrary pure state $|\Phi_{AB}\rangle$?
- What is the amount of entanglement in a mixed state ρ_{AB} ?

Entanglement Measures

- A measure of entanglement E must fullfill:

1. $E(\rho) \geq 0$ for $\forall \rho \in \mathscr{B}(\mathbb{H}_{\mathrm{A}} \otimes \mathbb{H}_{\mathrm{B}})$
2. $E(\sigma_{AB}) = 0$ if $\sigma_{\mathrm{AB}} = \sum_{\mathrm{i}} \mathrm{p_i} \sigma_{\mathrm{i}}^{\mathrm{A}} \otimes \sigma_{\mathrm{i}}^{\mathrm{B}}$, that is, if the state is separable
3. $E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) \leq E(\rho)$
4. Given a LOCC map Λ, $E(\Lambda(\rho)) \leq E(\rho)$
5. (*) Convexity: it may happen that $E(\sum p_i \rho_i) \leq \sum p_i E(\rho_i)$
6. (*) Additivity $E(\rho^{\otimes n}) = nE(\rho)$

- Remarks: (i) Convexity and Additivity are not necessary !
- (ii) There are many different entanglement measures and normally they are not equivalent!

Entanglement of pure states

Definition: The entanglement entropy is the standard entanglement measure used for bipartite pure state $|\psi\rangle_{AB}$

$$E(|\psi\rangle_{AB}) = S(\rho_A) = S(\rho_B)$$

where $S(\rho) = -Tr\rho \log(\rho)$ is the von Neumann entropy and

$\rho_A(\rho_B)$ are the reduced density matrices, i.e. $\rho_A = Tr_B(|\Psi\rangle_{AB}\langle\Psi|)$

Entanglement of pure states

Remarks:

- if $|\psi\rangle_{AB} = \Phi_A \otimes \varphi_B \Rightarrow E(|\psi\rangle_{AB}) = 0$ (product states have zero entanglement)
- if $|\Psi\rangle_{AB} = \sum_{i=1}^{M} \sqrt{\lambda_i}\,|e_i\rangle|f_i\rangle \Rightarrow E(|\Psi\rangle_{AB}) = -\sum \lambda_i \log \lambda_i$ (Shannon entropy)
- if $|\psi\rangle_{AB} = |\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \Rightarrow E(|\Psi^-\rangle_{AB}) = 1$ (an e-bit)
- if $|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle \Rightarrow E(\Psi^+\rangle_{AB}) = \log_2 d$
- If the pure state is N-multipartite $|\Psi\rangle_{1,2,..N}$ we can always calculate the entanglement entropy of a given bipartite splitting, i.e. $E(|\Psi\rangle_{AB})$ where AB is any bipartite splitting of the N parties

Entanglement of mixed states

Recall: To every ensemble of quantum states $\{p_i, |\psi_i\rangle\}$ one can associate a density operator $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \in \mathscr{B}(\mathbb{H})$.

Entanglement measures: convex roof extensions!

Entanglement of Formation E_{oF}

Definition: Given a bipartite mixed state ρ_{AB}, the entanglement of formation is defined as:

$$E_F(\rho_{AB}) = \min_{\{p_i, |\psi^i\rangle_{AB}\}} \sum p_i E(|\psi^i\rangle_{AB})$$

Remarks: (i) The infimum is taken over all possible ensembles compatibles with the mixed state

Meaning: The entanglement of formation tell us on average how many entanglement is need

Entanglement of mixed states

Entanglement of Formation E_{oF}

$$E_F(\rho_{AB}) = \min_{\{p_i, |\psi^i\rangle_{AB}\}} \sum p_i E(|\psi^i\rangle_{AB})$$

The convex roof optimization is VERY HARD to do, but for 2-qubit mixed states it can be computed via the concurrence.

Definition: The concurrence of a 2 qubit pure state $|\psi\rangle_{AB}$ is a measure of entanglement given by

$$C(|\psi\rangle_{AB}) = |\langle\psi_{AB}|\tilde{\psi}_{AB}\rangle| \text{ where } |\tilde{\psi}\rangle_{\mathrm{AB}} = \sigma_{\mathrm{y}} \otimes \sigma_{\mathrm{y}} |\psi\rangle^*_{\mathrm{AB}}$$

using the computational basis {|00>,|01>,|10>,|11>}

Entanglement of mixed states

Definition: The concurrence of a 2-qubit mixed state ρ_{AB} is a measure of entanglement given by

$$C(\rho_{AB}) = min(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4)$$

where λ_i are the eigenvalues in decreasing order of the operator $R = \sqrt{\sqrt{\rho_{AB}}\tilde{\rho}_{AB}\sqrt{\rho_{AB}}}$ where $\tilde{\rho}_{AB} = (\sigma_y \otimes \sigma_y)\rho^*_{AB}(\sigma_y \otimes \sigma_y)$

Theorem: The entanglement of formation of a 2-qubit mixed state ρ_{AB} is

$$E(\rho_{AB}) = F(C(\rho_{AB})) = h[\frac{1+\sqrt{1-C^2}}{2}]$$

and $h[x] = -x\log x - (1-x)\log(1-x)$

Entanglement of mixed states: entanglement cost and entanglement distillation

Entanglement cost and entanglement of distillation and two dual measures defined in the assymptotic limit. How many singlets do I need to prepare a bipartite state and how many singlets can I distill from a given state ρ_{AB} if I have many copies of the state.

Definition: The entanglement cost of a mixed state ρ_{AB} denoted by $E_c(\rho_{AB})$ is the infimum over all sequences of LOCC protocols such that given m-copies of the singlet state $|\Psi^-\rangle_{AB}^{\otimes m}$

$|\Psi^-\rangle_{AB}^{\otimes m} \underset{L \in LOCC}{\rightarrow} \sigma$ such that $\mathrm{D}(\rho_{\mathrm{AB}}^{\otimes \mathrm{n}}, \sigma) \underset{\mathrm{n}\rightarrow\infty}{\rightarrow} 0$ where D is a proper distance.

The entanglement cost of ρ_{AB} is defined as

$$E_c(\rho_{AB}) = \min_{L \in LOCC} \left(\lim_{n\rightarrow\infty} \frac{m}{n} \right)$$

$$E_c(\rho_{AB}) = \lim_{n\rightarrow\infty} \frac{E_F(\rho_{AB}^{\otimes n})}{n}$$

in simple words if defines the number e -bits one needs to create a entangled state σ which is the closest to the one we could achieved if we had n copies of our state using only LOCC operations.   can obtain   per input copy by LOCC operations

fr

Entanglement of mixed states: entanglement cost and entanglement distillation

. **Definition**: The entanglement of destillation of a mixed state ρ_{AB} denoted by $E_D(\rho_{AB})$ is the suprem over all sequences of LOCC protocols L such that given n-copies of our state $\rho_{AB}^{\otimes n}$ we approach a state whose distance to $|\Psi^-\rangle_{AB}^{\otimes m}$ singlets is zero in the assymptotic limit. If this is not possible $E_D = 0$. The entanglement of distillation is the supremum over all possible destillation rates. The rate of distillation is

The entanglement distillation of ρ_{AB} is defined as

$$E_D(\rho_{AB}) = \max_{L \in LOCC} \left(\lim_{n \to \infty} \frac{m}{n} \right)$$

where $D(|\Psi^-\rangle^{\otimes m}, \sigma_n) \underset{n\to\infty}{\rightarrow} 0$

, $\rho_{AB}^{\otimes n}$

Entanglement cost and entanglement distillation

Interpretation: In the limit of large n, Alice and Bob can destill m singlets $|\Psi^-\rangle_{AB}^{\otimes m}$ from n copies of their state, using only LOCC operations.

The entanglement of destillation is the suprem over all the set of LOCC operations

Theorem The entanglement of destillation is always smaller equal to the entanglement cost

$$E_D(\rho_{AB}) \leq E_c(\rho_{AB})$$

Entanglement of mixed states

Negativity

We introduce a last measure of entanglement whose meaning will will be clearer in the next slides.

Definition: The negativity of a shared quantum systems ρ_{AB} is the absolute sum of the negative eigenvalues of the partial transpose density matrix

$$\mathcal{N}(\rho_{AB}) = \frac{||\rho_{AB}^{T_B}|| - 1}{2} \text{ where } ||A|| = Tr(\sqrt{A^{\dagger}A})$$

Entanglement Criteria

To determine if a mixed state ρ_{AB} is entangled or separable is, in general, a NP-hard Problem (meaning not possible to solve in some cases).

Entanglement criteria provide necessary although not sufficient conditions.

Operational entanglement criteria

Definition: Let ρ_{AB} be a bipartite density matrix that can be expressed as

$$\rho_{AB} = \sum_{\substack{1 \le i,j \le d_A \\ 1 \le \mu,\nu \le d_B}} \rho_{ij}^{\mu\nu} (|i\rangle\langle j|)_A \otimes |\mu\rangle\langle\nu|_B)$$

the partial transpose of the density matrix ρ_{AB} with respect to system A is

$$\rho_{AB}^{T_A} = \sum_{\substack{1 \le i,j \le d_A \\ 1 \le \mu,\nu \le d_B}} \rho_{ij}^{\mu\nu} (|j\rangle\langle i|)_A \otimes |\mu\rangle\langle\nu|_B)$$

A similar definition exist for the partial transpose w.r.t subsystem B

Entanglement Criteria

Theorem: PPT criterion. If a state ρ_{AB} is separable, then $\rho_{AB}^{T_A} \geq 0$ and $\rho_{AB}^{T_B} = (\rho_{AB}^{T_A})^T \geq 0$

Proof: Trivial applying partial transposition on a separable state. A state that fullfills their partial transposes are positive is called a PPT (positive partial transpose) state.

Recall: $\rho_{AB}^{T_A} \geq 0$ means its eigenvalues are all larger or equal zero.

Theorem: If $dim(\mathbb{H}_A) \times dim(\mathbb{H}_B) \leq 6$, PPT is sufficient and necessary to proof the state is separable.

In higher dimensions, PPT criterion is NECESSARY for separability but not SUFFICIENT, meaning that there are states that are entangled and fulfill that $\rho_{AB}^{T_A} \geq 0$ and $\rho_{\mathrm{AB}}^{\mathrm{T_B}} \geq 0$.

Entanglement Criteria

Theorem: Entropy entanglement criterion. If a state ρ_{AB} is separable, then

$$S(\rho_{AB}) \geq S(\rho_A) \;\text{ and }\; \mathrm{S}(\rho_{\mathrm{AB}}) \geq \mathrm{S}(\rho_{\mathrm{B}})$$

where $S(\rho) = -Tr(\rho \log \rho)$ is the von Neumann entropy of the state.

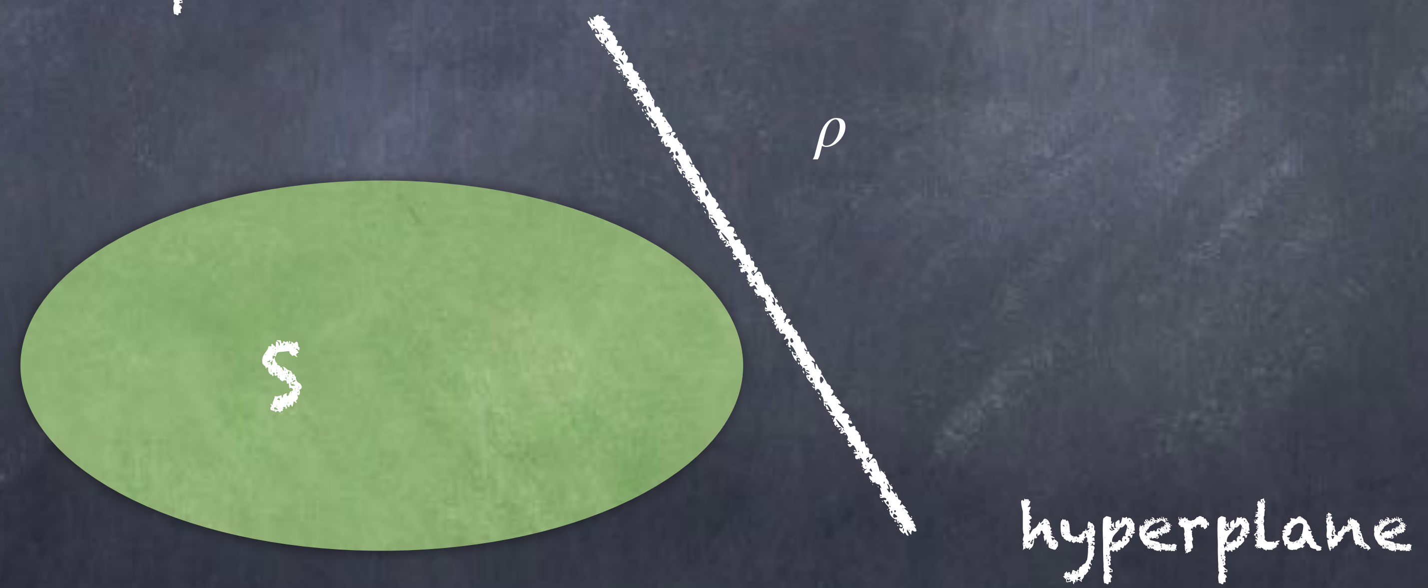
From all operationa entanglement criteria, PPT is probably the strongest but there are entangled states that are detected by the majorization or by entropy criterion that are not detected by PPT.

Non operational Entanglement Criteria

There are entanglement criteria that depend on the state we consider, for that reason they are called non-operational criteria

Lemma: $Tr(\rho_{AB}^{T_A}\sigma_{AB}) = Tr(\rho_{AB}\sigma_{AB}^{T_A})$

Theorem: Han-Banach theorem. Let S be a convex compatct set in a finite dimensional Banach space. Let ρ be a point with $\rho \notin S$ then there exist a hyperplane that separates ρ from S

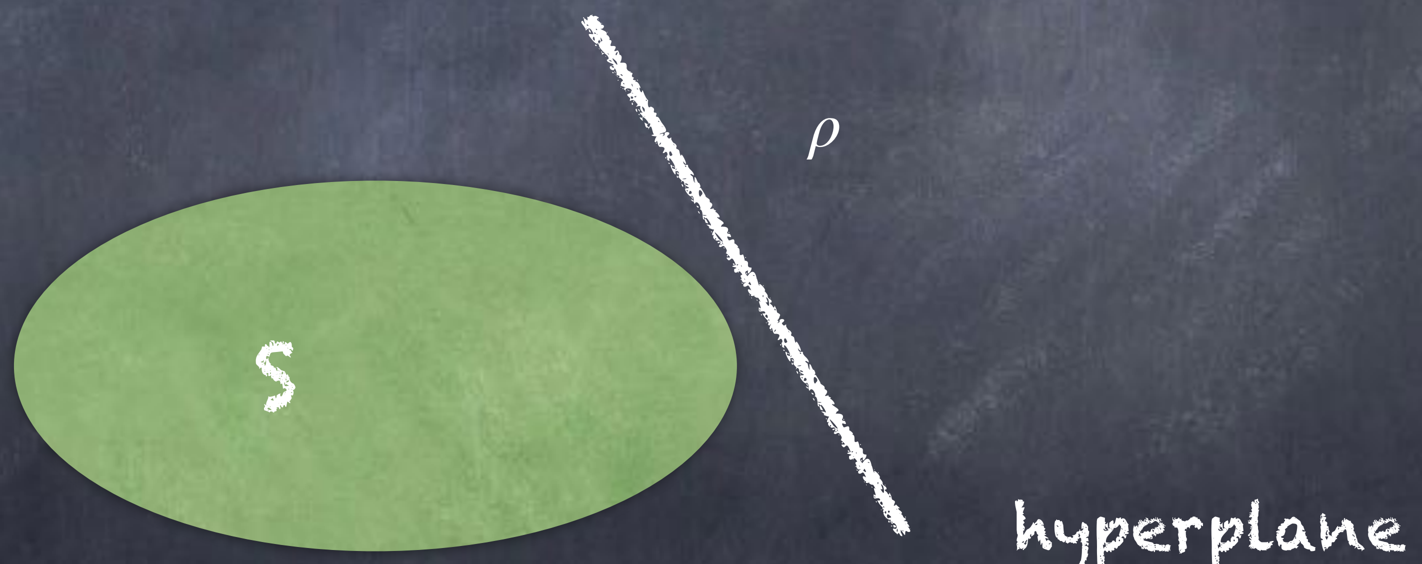


Entanglement witness

Definition: An Hermitian operators (observable) W is called an entanglement witness (EW) if and only if

1. $Tr(W\rho_S) \geq 0 \ \ \forall \rho \in S$ where S is the set of separable states

2. There exist at least one entangled state ρ such that $Tr(W\rho) < 0$



Entanglement witness

Definition: An entanglement witness is called decomposable if and only if there exsist operators P and Q such that

$$W = P + Q^{T_A} \quad \text{with} \quad \mathrm{P, Q} \geq 0$$

Lemma: A decomposable entanglement witness cannot detect PPT entangled states

Theorem:

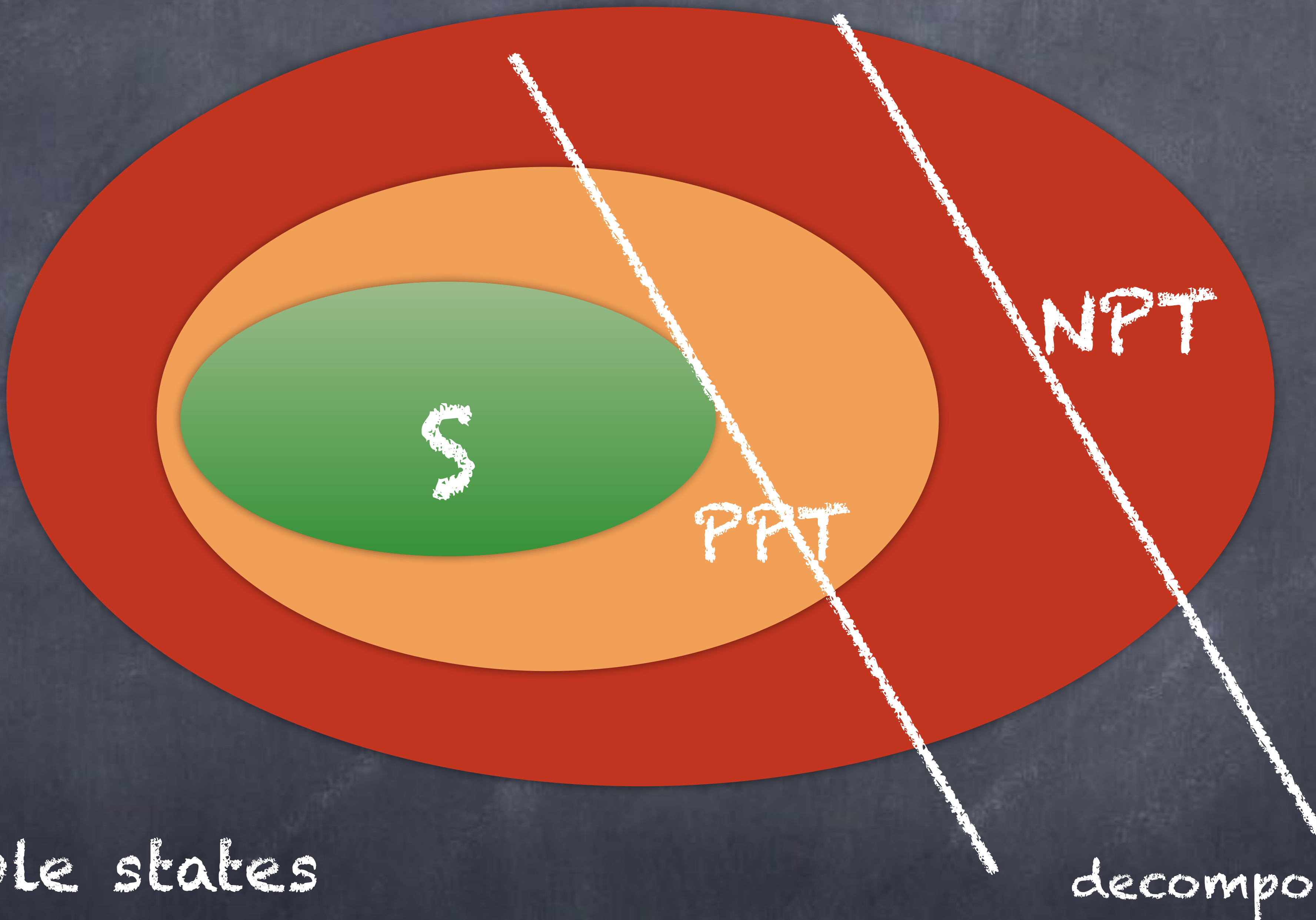
1. ρ is entangled if and only if there exist a witness W that detects it: $Tr(W\rho) < 0$.

2. ρ is an entangled PPT state if and only if there exist a non decomposable entanglement witness that detects it

3. σ is a separable state if and only if $Tr(W\sigma) \geq 0$ for all entanglement witnesses.

Entanglement witness

The structure of the space of quantum states



S sepable states

PPT entangled states

NPT entangled states

Entanglement witness

Example: Let us construct a witness for a bipartite pure maximally entangled state. We take $|\Phi^+\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

A witness operator is immediate construct as $W = Q^{T_A} = (|\Phi^+\rangle\langle\Phi^+|)^{T_A}$

$$Q = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 1 & 1/2 \end{pmatrix} \qquad Q^{T_A} = \begin{pmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 1/2 \end{pmatrix} = (1 - 2|\Psi^-\rangle\langle\Psi^-|)$$

To show that W is a witness we need to show that

Entanglement witness

To show that $W = Q^{T_A} = (|\Phi^+\rangle\langle\Phi^+|)^{T_A}$ is a witness we need to show

(i) $\mathrm{Tr}(W\rho_{\mathrm{sep}}) \geq 0$, this is equivalent to show that $\mathrm{Tr}(W|e,f\rangle\langle e,f|) = \langle e,f|W|e,f\rangle \geq 0$. It suffices to write $|e\rangle = a_o|0\rangle + b_0|1\rangle$, and $|f\rangle = a_1|0\rangle + b_1|1\rangle$, with $a_i, b_i \in \mathbb{C}$

(ii) There exist one entangled state such that $\mathrm{Tr}(W\rho_e) < 0$. Choose $\rho_e = |\Psi^-\rangle\langle\Psi^-|$. Trivially $\mathrm{Tr}(W\rho_e) = -1$

$$Q^{T_A} = \begin{pmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 1/2 \end{pmatrix} = (1 - 2|\Psi^-\rangle\langle\Psi^-|)$$