Entanglement Detection

Module 2 of QIC 890 and 891
May 21 – June 2, 2014

Nathaniel Johnston

Contents

Lecture 1

Separability and Entanglement: The Basics

Quantum entanglement is one of the key resources in quantum information theory, being a necessary resource in almost all quantum information processing tasks. The question arises, however, how we can be sure that the state of our quantum system is actually entangled. The goal of this module is to investigate this question.

Specifically, we will investigate methods for proving that a state is entangled in the setting where we have a complete (classical) description of the state of our system (e.g., the state that we wish to determine is entangled was arrived at via a calculation, not an experiment... alternatively, we are fortunate enough that we can perform full state tomography and learn everything about the state of our system).

References to specific results will occasionally be provided within the course notes, especially when we don't actually prove or delve too deeply into the results ourselves. Two general references that might be of use to you throughout this module are:

- O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474:1–75, 2009. arXiv:0811.2803 [quant-ph]

- R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865–942, 2009. arXiv:quant-ph/0702225

1.1 Pure State Entanglement

A pure state $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ is called *separable* (or sometimes a *product state*) if it can be written in the form $|v\rangle = |a\rangle \otimes |b\rangle$ for some $|a\rangle \in \mathbb{C}^n$ and $|b\rangle \in \mathbb{C}^m$. Otherwise, $|v\rangle$ is called *entangled*.

The Schmidt decomposition theorem provides a simple method for determining whether a pure state is separable or entangled (and if it is entangled, the theorem lets us see "how" entangled it is).

Theorem 1.1.1 (Schmidt decomposition)**.** *For any unit vector $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ there exists an integer $1 \leq r \leq \min\{n, m\}$, strictly positive real scalars $\{\gamma_i\}_{i=1}^r$ with $\sum_{i=1}^r \gamma_i^2 = 1$, and orthonormal sets of vectors $\{|a_i\rangle\}_{i=1}^r \subset \mathbb{C}^n$ and $\{|b_i\rangle\}_{i=1}^r \subset \mathbb{C}^m$ such that*

$$|v\rangle = \sum_{i=1}^r \gamma_i |a_i\rangle \otimes |b_i\rangle.$$

Before proving the theorem, we offer some notes on terminology:

- The integer r is called the *Schmidt rank* of $|v\rangle$, and $r = 1$ if and only if $|v\rangle$ is separable.
- The scalars $\{\gamma_i\}_{i=1}^r$ are called the *Schmidt coefficients* of $|v\rangle$, and they are the nonzero square roots of the eigenvalues of $\mathrm{Tr}_A(|v\rangle\langle v|)$.
- Every piece of Theorem 1.1.1 is easily computed.

Proof. Assume that $n \leq m$, as it will be clear how to modify the proof if the opposite inequality holds. Begin by defining a linear map $\Gamma : \mathbb{C}^n \otimes \mathbb{C}^m \to M_{n,m}$ by $\Gamma(|ij\rangle) = |i\rangle\langle j|$. This map is easily seen to be a bijection between these two spaces.

By the singular value decomposition, there exist unitary matrices $U \in M_n$, $V \in M_m$, and a diagonal matrix $D \in M_{n,m}$ with nonnegative entries such that

$$\Gamma(|v\rangle) = UDV.$$

Performing this matrix multiplication gives

$$\Gamma(|v\rangle) = \sum_{i=1}^r \gamma_i |a_i\rangle\overline{\langle b_i|},$$

where r is the rank of $\Gamma(|v\rangle)$, γ_i is the i-th nonzero diagonal entry of D, $|a_i\rangle$ is the i-th column of U, and $\overline{\langle b_i|}$ is the i-th row of V. Since U and V are both unitary, the sets $\{|a_i\rangle\}_{i=1}^r$ and $\{|b_i\rangle\}_{i=1}^r$ are orthonormal. Furthermore, a simple calculation reveals that

$$\Gamma\Big(\sum_{i=1}^r \gamma_i|a_i\rangle \otimes |b_i\rangle\Big) = \sum_{i=1}^r \gamma_i|a_i\rangle\overline{\langle b_i|} = \Gamma(|v\rangle).$$

It follows from the fact that Γ is a bijection that

$$|v\rangle = \sum_{i=1}^r \gamma_i|a_i\rangle \otimes |b_i\rangle,$$

as desired. To see that $\sum_{i=1}^r \gamma_i^2 = 1$, simply notice that $1 = \||v\rangle\|^2 = \langle v|v\rangle = \sum_{i=1}^r \gamma_i^2$. □

The proof of Theorem 1.1.1 tells us how to determine whether or not $|v\rangle$ is separable: it is separable if and only if the matrix $\Gamma(|v\rangle)$ has rank 1. For example, if $|v\rangle = |00\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ (which is clearly separable) then we have

$$\Gamma(|v\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

which has rank 1. On the other hand, if $|v\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is a Bell state then

$$\Gamma(|v\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

which has rank 2, so $|v\rangle$ is entangled.

1.2 Mixed State Entanglement

In the case of mixed states, we say that $\rho \in M_n \otimes M_m$ is *separable* if it can be written as a convex combination of separable pure states:

$$\rho = \sum_{i=1}^k p_i|v_i\rangle\langle v_i|, \tag{1.1}$$

where $|v_i\rangle = |a_i\rangle \otimes |b_i\rangle$ for all i, $0 \leq p_i \leq 1$ for all i, and $\sum_i p_i = 1$. If ρ cannot be written in the form (1.1) then it is called *entangled*. We note that the set of separable states is both closed and convex.

In the previous section we saw that we can easily determine whether or not a given pure state is entangled. However, the same is *not* true of mixed states: determining whether or not a given mixed state ρ is separable is NP-hard [Gur03], so we don't expect that we'll be able to efficiently solve this problem in complete generality. Instead, we try to find one-sided tests (called *separability criteria*) that are able to prove separability or entanglement for certain subsets of states.

1.2.1 The Partial Transpose

The most well-known separability criterion is based on the *partial transpose* map, which applies the usual matrix transpose to one half of the space $M_n \otimes M_m$. That is, the partial transpose is the linear map $id \otimes T$ that acts on $M_n \otimes M_m$ as follows: $(id \otimes T)(A \otimes B) = A \otimes B^T$.

The following proposition shows that the partial transpose can be used to detect entanglement in some quantum states.

Proposition 1.2.1 (Positive partial transpose (PPT) criterion)**.** *Let $\rho \in M_n \otimes M_m$ be separable. Then $(id \otimes T)(\rho)$ is positive semidefinite.*

Proof. Since ρ is separable, we can write $\rho = \sum_i p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|$. Then

$$(id \otimes T)(\rho) = \sum_i p_i |a_i\rangle\langle a_i| \otimes (|b_i\rangle\langle b_i|)^T,$$

which is positive semidefinite as a result of each $|a_i\rangle\langle a_i|$ and $(|b_i\rangle\langle b_i|)^T$ being positive semidefinite. □

Note that the contrapositive of Proposition 1.2.1 is what is used in practice: if $(id \otimes T)(\rho)$ is *not* positive semidefinite then we can conclude that ρ is entangled. For example, if

$$\rho = \frac{1}{4}\begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \end{bmatrix} \in M_2 \otimes M_2$$

then we can compute

$$(id \otimes T)(\rho) = \frac{1}{4}\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix},$$

which has eigenvalues $\frac{1}{2}, \frac{1}{2}, \frac{1}{4}$, and $\frac{-1}{4}$ and is thus not positive semidefinite. It follows from Proposition 1.2.1 that ρ is entangled.

However, if $(id \otimes T)(\rho)$ is positive semidefinite (in which case ρ is said to have *positive partial transpose (PPT)*) then what can we say about whether ρ is separable or entangled? In general, nothing. However, in some special cases...

Theorem 1.2.2. *Let $\rho \in M_n \otimes M_m$ with $nm \leq 6$. Then ρ is separable if and only if $(id \otimes T)(\rho)$ is positive semidefinite.*

In other words, the converse of Proposition 1.2.1 holds in small dimensions. The proof of Theorem 1.2.2 is extremely technical [Stø63, Wor76], so we will just treat it as a magical gift from operator theorists.

1.2.2 Positive Maps and Entanglement Witnesses

Recall that quantum channels are represented by linear maps $\Phi : M_m \to M_n$ that are *completely positive*: i.e., they satisfy $(id_k \otimes \Phi)(\rho) \geq 0$ for all $k \geq 1$ and all $\rho \in M_k \otimes M_m$. Also recall that Φ is completely positive if and only if its *Choi matrix*, defined by

$$J(\Phi) \overset{\text{def}}{=} m(id \otimes \Phi)(|\psi^+\rangle\langle\psi^+|), \quad \text{where} \quad |\psi^+\rangle := \frac{1}{\sqrt{m}}\sum_{i=0}^{m-1} |i\rangle \otimes |i\rangle,$$

is positive semidefinite. In this section, we won't be interested in completely positive maps, but rather maps that are just *positive*. That is, maps $\Phi : M_m \to M_n$ with the property that $\Phi(\rho) \geq 0$ for all $\rho \in M_m$.

We have already seen one linear map that is positive but not completely positive: the transpose map $T : M_m \to M_m$. To see that it is positive, just recall that the eigenvalues of X^T are the same as the eigenvalues of X. To see that it is not completely positive, notice that its Choi matrix is

$$J(T) = (id \otimes T)\Big(\sum_{i,j=0}^{m-1} |i\rangle\langle j| \otimes |i\rangle\langle j|\Big) = \sum_{i,j=0}^{m-1} |i\rangle\langle j| \otimes |j\rangle\langle i|.$$

It is then straightforward to verify that the operator $J(T)$ is unitary (i.e., $J(T)^\dagger J(T) = I$) and Hermitian, so all of its eigenvalues are ± 1. Since it is not the identity operator, it must have at least 1 negative eigenvalue, so $J(\Phi)$ is not positive semidefinite and the transpose map is not completely positive.

It seems natural to ask what properties the Choi matrix of a positive map must have. This question is answered by the following proposition.

Proposition 1.2.3. *A linear map $\Phi : M_m \to M_n$ is positive if and only if $\mathrm{Tr}(J(\Phi)\sigma) \geq 0$ for all separable $\sigma \in M_m \otimes M_n$.*

Proof. To prove the "only if" direction, first notice that we can use convexity of the set of separable states to see that it suffices to consider the case when $\sigma = |a\rangle\langle a| \otimes |b\rangle\langle b|$. Then we have:

$$\begin{aligned}
\mathrm{Tr}\Big(J(\Phi)(|a\rangle\langle a| \otimes |b\rangle\langle b|)\Big) &= (\langle a| \otimes \langle b|)J(\Phi)(|a\rangle \otimes |b\rangle) \\
&= \sum_{i,j=0}^{m-1} (\langle a| \otimes \langle b|)\Big(|i\rangle\langle j| \otimes \Phi(|i\rangle\langle j|)\Big)(|a\rangle \otimes |b\rangle) \\
&= \langle b|\Phi\Big(\sum_{i,j=0}^{m-1} \langle a|i\rangle|i\rangle\langle j|a\rangle\langle j|\Big)|b\rangle \\
&= \langle b|\Phi\Big(\overline{|a\rangle\langle a|}\Big)|b\rangle \\
&\geq 0.
\end{aligned}$$

The "if" direction can be proved by using the exact same argument as above in reverse. □

The Choi matrices of positive maps are actually given a special name—if a Hermitian operator $W \in M_m \otimes M_n$ satisfies $\mathrm{Tr}(W\sigma) \geq 0$ for all separable $\sigma \in M_m \otimes M_n$ but has $\mathrm{Tr}(W\rho) < 0$ for some (necessarily entangled) $\rho \in M_m \otimes M_n$ then W is called an *entanglement witness*. By Proposition 1.2.3, a linear map is positive but not completely positive if and only if its Choi matrix is an entanglement witness. The reason for our interest in positive maps and entanglement witnesses is the following theorem.

Theorem 1.2.4. *Let $\rho \in M_m \otimes M_n$. The following are equivalent:*

a) *ρ is separable;*

b) *$\mathrm{Tr}(W\rho) \geq 0$ for all entanglement witnesses $W \in M_m \otimes M_n$; and*

c) *$(id \otimes \Phi)(\rho) \geq 0$ for all positive linear maps $\Phi : M_n \to M_m$.*

Proof. The implication **a)** $\implies$ **c)** is straightforward and follows the exact same logic that we saw with the partial transpose map: if ρ is separable then we can write

$$\rho = \sum_i p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|.$$

Then

$$(id \otimes \Phi)(\rho) = \sum_i p_i |a_i\rangle\langle a_i| \otimes \Phi(|b_i\rangle\langle b_i|) \geq 0,$$

where positive semidefiniteness follows from the fact that Φ is positive so $\Phi(|b_i\rangle\langle b_i|) \geq 0$ for all i.

To see that **c)** $\implies$ **b)**, notice that $(id \otimes \Phi)(\rho) \geq 0$ implies

$$\begin{aligned} 0 &\leq \langle \psi^+|(id \otimes \Phi)(\rho)|\psi^+\rangle \\ &= \mathrm{Tr}\Big(|\psi^+\rangle\langle\psi^+|(id \otimes \Phi)(\rho)\Big) \\ &= \mathrm{Tr}\Big((id \otimes \Phi^\dagger)(|\psi^+\rangle\langle\psi^+|)\rho\Big). \end{aligned}$$

Now define $W := (id \otimes \Phi^\dagger)(|\psi^+\rangle\langle\psi^+|)$ and notice that we have $\mathrm{Tr}(W\rho) \geq 0$. Since Φ is positive, $\Phi^\dagger$ is positive too (prove this yourself), so Proposition 1.2.3 implies that W is an entanglement witness. Furthermore, *every* entanglement witness has this form for some positive Φ, so *b)* follows.

Finally, to see that **b)** $\implies$ **a)**, we prove the contrapositive that ρ being entangled implies that there exists an entanglement witness W such that $\mathrm{Tr}(W\rho) < 0$. To this end recall that the set of separable states is closed and convex. By the separating hyperplane theorem, if ρ is entangled then there exists a Hermitian operator $H \in M_m \otimes M_n$ and a constant $c \in \mathbb{R}$ such that $\mathrm{Tr}(H\rho) < c$, but $\mathrm{Tr}(H\sigma) \geq c$ for all separable σ. It is straightforward to verify that $W := H - cI$ is an entanglement witness, as desired. □

On the one hand, positive maps can be used to completely characterize entanglement, as seen above. On the other hand, we only know a handful of positive maps, and determining whether or not a linear map is positive is also NP-hard. For now, let's expand our arsenal of positive maps a little bit.

The Reduction Map

One of the most well-known positive maps other than the transpose map is the *reduction map*, which is the positive linear map $R : M_n \to M_n$ defined by

$$R(X) \stackrel{\text{def}}{=} \mathrm{Tr}(X)I - X.$$

We now show that the reduction map can be used to detect entanglement in some states.

Proposition 1.2.5. *If $n \geq 2$ then the reduction map $R : M_n \to M_n$ is positive but not completely positive.*

Proof. To see that R is positive, suppose that $X \geq 0$. If we use $\{\lambda_i\}_{i=1}^n$ to denote the eigenvalues of X, then the eigenvalues of $R(X) = \mathrm{Tr}(X)I - X$ are $\{\mathrm{Tr}(X) - \lambda_i\}_{i=1}^n$. Since $\mathrm{Tr}(X) = \sum_{j=1}^n \lambda_j \geq \lambda_i$ for all $1 \leq i \leq n$, it follows that $R(X) \geq 0$, as desired.

Try to prove that R is not completely positive yourself (what is $J(R)$?). □

In spite of Proposition 1.2.5, the reduction map is not actually used in practice to prove that states are entangled, since it turns out that the transpose map is always a better choice (i.e., every time that the reduction map detects entanglement in a state, so does the transpose map). You will prove this fact in Exercise 1. Nonetheless, the reduction map has some interesting theoretical properties.

The Choi Map

Note that it was very easy to prove that the reduction map is positive (and it is also very easy to prove that the transpose map is positive). We now investigate another positive map to give you a more "realistic" view of what it is typically like to prove that a given map is positive.

We now introduce the *Choi map*, which is the positive map $\Phi_C : M_3 \to M_3$ defined as follows:

$$\Phi_C(X) \stackrel{\text{def}}{=} \begin{bmatrix} x_{11} + x_{22} & -x_{12} & -x_{13} \\ -x_{21} & x_{22} + x_{33} & -x_{23} \\ -x_{31} & -x_{32} & x_{33} + x_{11} \end{bmatrix}.$$

Notice that Φ_C is quite similar to the reduction map on 3×3 matrices—all that has changed is that the diagonal entries are permuted.

Theorem 1.2.6. *The Choi map $\Phi_C : M_3 \otimes M_3$ is positive but not completely positive.*

Proof. You can check that it is not completely positive yourself by computing $J(\Phi_C)$. We focus only on proving that it is positive.

By convexity of the set of positive-semidefinite matrices, it suffices to show that $\Phi_C(|v\rangle\langle v|) \geq 0$ for all pure states $|v\rangle \in \mathbb{C}^3$. If we write $|v\rangle = [v_1, v_2, v_3]^T$ then what we want to show is that

$$\Phi_C(|v\rangle\langle v|) = \begin{bmatrix} |v_1|^2 + |v_2|^2 & -v_1\overline{v_2} & -v_1\overline{v_3} \\ -\overline{v_1}v_2 & |v_2|^2 + |v_3|^2 & -v_2\overline{v_3} \\ -\overline{v_1}v_3 & -\overline{v_2}v_3 & |v_3|^2 + |v_1|^2 \end{bmatrix} \geq 0. \qquad (1.2)$$

Recall that we can prove that the matrix (1.2) is positive semidefinite (and hence Φ_C is positive) by checking that all of its principal minors are nonnegative (recall that a *principal minor* of a matrix X is the determinant of a matrix obtained by deleting some k rows and the same k columns from X). This is basically just grunt work, but maybe it helps us dig up some long-forgotten linear algebra, so let's do it:

There are three 1×1 principal minors of $\Phi_C(|v\rangle\langle v|)$:

$$|v_1|^2 + |v_2|^2, \quad |v_2|^2 + |v_3|^2, \quad \text{and} \quad |v_3|^2 + |v_1|^2,$$

which are clearly nonnegative.

There are three 2×2 principal minors of $\Phi_C(|v\rangle\langle v|)$:

$$\begin{aligned} \det\left(\begin{bmatrix} |v_1|^2 + |v_2|^2 & -\overline{v_1}v_2 \\ -v_1\overline{v_2} & |v_2|^2 + |v_3|^2 \end{bmatrix}\right) &= (|v_1|^2 + |v_2|^2)(|v_2|^2 + |v_3|^2) - |v_1|^2|v_2|^2 \\ &= |v_1|^2|v_3|^2 + |v_2|^4 + |v_2|^2|v_3|^2 \\ &\geq 0. \end{aligned}$$

The calculation for the other two 2×2 principal minors is almost identical and is thus omitted.

Finally, there is just one 3×3 principal minor of $\Phi_C(|v\rangle\langle v|)$:

$$\begin{aligned} \det\big(\Phi_C(|v\rangle\langle v|)\big) &= (|v_1|^2 + |v_2|^2)(|v_2|^2 + |v_3|^2)(|v_3|^2 + |v_1|^2) - 2|v_1|^2|v_2|^2|v_3|^2 \\ &\quad - (|v_1|^2 + |v_2|^2)|v_2|^2|v_3|^2 - (|v_2|^2 + |v_3|^2)|v_1|^2|v_3|^2 \\ &\quad - (|v_3|^2 + |v_1|^2)|v_1|^2|v_2|^2 \\ &= |v_1|^2|v_2|^4 + |v_2|^2|v_3|^4 + |v_3|^2|v_1|^4 - 3|v_1|^2|v_2|^2|v_3|^2. \end{aligned}$$

In order to show that this quantity is nonnegative, we define $x := |v_1|^2, y := |v_2|^2$, and $z := |v_3|^2$, and solve the following optimization problem:

$$\begin{aligned} \text{minimize:} \quad & xy^2 + yz^2 + zx^2 - 3xyz \\ \text{subject to:} \quad & x, y, z \geq 0 \\ & x + y + z = 1. \end{aligned}$$

This is a standard optimization problem that could be solved in a multivariable calculus course. Since the optimization takes place over a closed and bounded set, it suffices to (1) plug the constraint $x + y + z = 1$ into the objective function to eliminate one of the variables, (2) check the value of the objective function on the boundary of that set being optimized over, and (3) check the value of the objective function at its critical points.

All of this is just a (messy and somewhat long) calculation—you can do it if you so desire, or you can take my word for it that the minimum value really is 0, which shows that Φ_C is positive. Alternatively, if you don't trust me you can take WolframAlpha's word for it. □

Exercises

Exercise 1. Let $R : M_n \to M_n$ be the reduction map introduced in Section 1.2.2 and let $\rho \in M_n \otimes M_n$ be a mixed state.

a) Prove that if $(id_n \otimes R)(\rho) \not\geq 0$ then $(id_n \otimes T)(\rho) \not\geq 0$. That is, show that the transpose map can detect entanglement in every state ρ that the reduction map can. [Hint: Show that the map $R \circ T$ is completely positive.]

b) Prove that, in the $n = 2$ case, $(id_2 \otimes R)(\rho) \not\geq 0$ if and only if $(id_2 \otimes T)(\rho) \not\geq 0$. [Hint: Show that the map $R \circ T$ is its own inverse when $n = 2$.]

Lecture 2

Creating PPT Entangled States

We saw in the previous lecture that the partial transpose provides one of the simplest and most useful tests for proving that a state is entangled. However, in systems larger than $M_2 \otimes M_3$, this test is only one-sided: if the partial transpose of a state has a negative eigenvalue then we know that it is entangled, but if it has positive partial transpose then it may or may not be entangled. In this lecture we present one method for creating states that are entangled yet have positive partial transpose. In future lectures, we will develop tests that let us detect the entanglement in these states.

2.1 Multipartite Entanglement

In Lecture 1, we discussed the problem of determining whether or not a given quantum state is separable in the *bipartite* case (i.e., the case of two subsystems). This question can also be asked in the *multipartite* setting (i.e., the case of an arbitrary (but finite) number of subsystems), and all of the definitions extend in the obvious ways. In particular, a pure state $|v\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ is separable if and only if there exists $|v^j\rangle \in \mathbb{C}^{n_j}$ for $1 \leq j \leq p$ such that

$$|v\rangle = |v^1\rangle \otimes |v^2\rangle \otimes \cdots \otimes |v^p\rangle.$$

Similarly, a mixed state $\rho \in M_{n_1} \otimes M_{n_2} \otimes \cdots \otimes M_{n_p}$ is separable if and only if we can write

$$\rho = \sum_{i=1}^{k} p_i |v_i\rangle\langle v_i|$$

for some separable pure states $\{|v_i\rangle\} \subset \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$.

However, even though the relevant definitions carry over to the multipartite setting without much thought, we will see in this lecture that it is not always straightforward to use bipartite separability criteria to determine multipartite separability.

2.2 Unextendible Product Bases

One method for creating PPT entangled states (and also demonstrating plenty of other strange entanglement phenomena) is by using *unextendible product bases (UPBs)*, which are sets $\mathcal{U} = \{|v_1\rangle, |v_2\rangle, \ldots, |v_s\rangle\} \subset \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ of product vectors satisfying the following two properties:

a) $\langle v_i | v_j \rangle = 0$ for all $1 \leq i \neq j \leq s$, and

b) there does not exist a product vector $|z\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ such that $\langle v_i | z \rangle = 0$ for all $1 \leq i \leq s$.

It is clear that the standard basis of $\mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ satisfies all of the requirements above and is thus a UPB. However, UPBs that span the entire space $\mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ will be completely useless for our purposes, so we ignore them and instead only consider UPBs that span a proper subspace of $\mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ (we call such UPBs *nontrivial*).

2.2.1 Bipartite UPBs

It is perhaps not immediately clear that nontrivial UPBs even exist, so we start off with an example of one in the bipartite case. In particular, we define a set $\mathcal{U}_{\text{tiles}} = \{|v_1\rangle, \ldots, |v_5\rangle\} \subset \mathbb{C}^3 \otimes \mathbb{C}^3$ that we refer to as the “tiles”

UPB as follows:

$$|v_1\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle), \qquad |v_2\rangle = \frac{1}{\sqrt{2}}|2\rangle \otimes (|1\rangle - |2\rangle)$$
$$|v_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle, \qquad |v_4\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle$$
$$|v_5\rangle = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle) \otimes (|0\rangle + |1\rangle + |2\rangle).$$

To see that these five states form a UPB, we check the two defining properties given in the previous section. For property **a)**, you can just manually check that each state is orthogonal to every other state. For example, $|v_1\rangle$ is orthogonal to $|v_2\rangle$ and $|v_4\rangle$ on the first system and it is orthogonal to $|v_3\rangle$ and $|v_5\rangle$ on the second system.

For property **b)**, suppose for a contradiction that there exists a product state $|z\rangle = |z^1\rangle \otimes |z^2\rangle \in \mathbb{C}^3 \otimes \mathbb{C}^3$ such that $\langle v_i|z\rangle = 0$ for $1 \leq i \leq 5$. Then $|z\rangle$ must be orthogonal to at least 3 of the $|v_i\rangle$'s on either the first or second system (otherwise it would only be orthogonal to at most 2 states on each system, for a total of at most $2 + 2 = 4$ of the 5 states). That is, $|z^1\rangle$ must be orthogonal to at least 3 of the following states:

$$|0\rangle, |2\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \tag{2.1}$$

or $|z^2\rangle$ must be orthogonal to at least 3 of the following states:

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), |2\rangle, |0\rangle, \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle). \tag{2.2}$$

However, it is a straightforward calculation to show that any three states in (2.1) are linearly independent, and similarly for any three states in (2.2), which implies that no $|z^1\rangle$ or $|z^2\rangle$ satisfies the desired property. This is the contradiction that shows that property **b)** holds, so $\mathcal{U}_{\text{tiles}}$ really is a UPB.

Our First PPT Entangled State

Our primary interest in UPBs comes from the following proposition, which shows that every UPB can be used to construct a PPT entangled state.

Proposition 2.2.1. *Let $\mathcal{U} = \{|v_1\rangle, |v_2\rangle, \ldots, |v_s\rangle\} \subset \mathbb{C}^n \otimes \mathbb{C}^m$ be a UPB. Then the state*

$$\rho := \frac{1}{nm - s}(I - \sum_{i=1}^{s} |v_i\rangle\langle v_i|) \tag{2.3}$$

is PPT and entangled.

Proof. It is straightforward to see that this state is PPT: if we write $|v_i\rangle = |v_i^1\rangle \otimes |v_i^2\rangle$ then

$$\begin{aligned}(id \otimes T)(\rho) &= \frac{1}{nm - s}\Big(I - \sum_{i=1}^{s} |v_i^1\rangle\langle v_i^1| \otimes (|v_i^2\rangle\langle v_i^2|)^T\Big)\\ &= \frac{1}{nm - s}\Big(I - \sum_{i=1}^{s}(|v_i^1\rangle \otimes \overline{|v_i^2\rangle})(\langle v_i^1| \otimes \overline{\langle v_i^2|})\Big)\\ &\geq 0,\end{aligned}$$

where $\overline{|v_i^2\rangle}$ refers to the complex conjugate of $|v_i^2\rangle$ (in the same basis as the transpose was taken).

Why is the state (2.3) entangled? Suppose for a contradiction that ρ is separable, so we can find product states $\{|z_j\rangle\} \subset \mathbb{C}^n \otimes \mathbb{C}^m$ such that

$$\rho = \sum_{j=1}^{k} p_j |z_j\rangle\langle z_j|.$$

However, ρ is (up to scaling) the orthogonal projection onto the orthogonal complement of span$\{\mathcal{U}\}$. Thus $\langle v_i|z_j\rangle = 0$ for all $|v_i\rangle \in \mathcal{U}$ and for all $|z_j\rangle$, which contradicts unextendibility of $\mathcal{U}$. □

Since we have already constructed a UPB in $\mathbb{C}^3 \otimes \mathbb{C}^3$, it follows from Proposition 2.2.1 that we can create a PPT entangled state in $M_3 \otimes M_3$.

UPBs in Qubit–Qudit Systems

We already saw that there are no nontrivial UPBs in $\mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathbb{C}^2 \otimes \mathbb{C}^3$ (Why? What kind of mixed state would this let you construct?). We now show that the same result is true in $\mathbb{C}^2 \otimes \mathbb{C}^n$, regardless of n

Theorem 2.2.2. *Every unextendible product basis in $\mathcal{U} \subset \mathbb{C}^2 \otimes \mathbb{C}^n$ spans the full $2n$-dimensional space.*

Proof. Throughout this proof we assume that the system $\mathbb{C}^2$ is held by Alice and the system $\mathbb{C}^n$ is held by Bob. First note that, up to global phase (which is irrelevant), there is only one pure state orthogonal to any other given pure state in $\mathbb{C}^2$. We make use of this fact by sorting the members of $\mathcal{U}$ into disjoint subsets that are equal and orthogonal on Alice's system. More specifically, we write $\mathcal{U}$ in the following way:

$$\mathcal{U} = (P_1 \cup Q_1) \cup (P_2 \cup Q_2) \cup \cdots \cup (P_k \cup Q_k),$$

where

$$P_j := \Big\{|a_j\rangle \otimes |b_{j1}\rangle, |a_j\rangle \otimes |b_{j2}\rangle, \ldots, |a_j\rangle \otimes |b_{j\ell_j}\rangle\Big\} \quad \text{and}$$
$$Q_j := \Big\{|a_j^\perp\rangle \otimes |c_{j1}\rangle, |a_j^\perp\rangle \otimes |c_{j2}\rangle, \ldots, |a_j^\perp\rangle \otimes |c_{jr_j}\rangle\Big\}.$$

That is, we take some element of $\mathcal{U}$, place it into P_1, and then place in P_1 all other members of $\mathcal{U}$ that are equal to it on Alice's system. Then we place in Q_1 all members of $\mathcal{U}$ that are orthogonal to the members of P_1 on Alice's system. Then we pick any member of $\mathcal{U}$ that is in neither of P_1 or Q_1 and place it in P_2, and repeat this process until we have exhausted all of $\mathcal{U}$.

We now claim that

$$\mathrm{span}\{|b_{j1}\rangle, |b_{j2}\rangle, \ldots, |b_{j\ell_j}\rangle\} = \mathrm{span}\{|c_{j1}\rangle, |c_{j2}\rangle, \ldots, |c_{jr_j}\rangle\} \quad \forall\, j. \tag{2.4}$$

That is, we claim that the span of P_j and Q_j, when restricted to Bob's system, coincides for all $1 \leq j \leq k$. To see why this claim holds, fix j and suppose the contrary: suppose that there exists a state $|v\rangle \in \mathbb{C}^n$ such that

$$|v\rangle \in \mathrm{span}\{|b_{j1}\rangle, \ldots, |b_{j\ell_j}\rangle\} \quad \text{and} \quad |v\rangle \notin \mathrm{span}\{|c_{j1}\rangle, \ldots, |c_{jr_j}\rangle\}$$

(the argument is almost identical if $|v\rangle$ is in the right set but not the left set, so we omit it). Then we claim that the state $|a^\perp\rangle \otimes |v\rangle$ is orthogonal to every member of $\mathcal{U}$, which contradicts the fact that $\mathcal{U}$ is unextendible. To see this, note that $|a^\perp\rangle \otimes |v\rangle$ is orthogonal to every member of P_j on Alice's system, it is orthogonal to every member of Q_j on Bob's system since $|v\rangle \notin \mathrm{span}\{|c_{j1}\rangle, \ldots, |c_{jr_j}\rangle\}$, and it is orthogonal to every member of P_ℓ, Q_ℓ $(\ell \neq j)$ on Bob's system since $|v\rangle \in \mathrm{span}\{|b_{j1}\rangle, \ldots, |b_{j\ell_j}\rangle\}$.

We have thus proved that Equation (2.4) holds. We now define subspaces $S_j := \mathrm{span}\{|b_{j1}\rangle, \ldots, |b_{j\ell_j}\rangle$ for $1 \leq j \leq k$ and we note that these subspaces are mutually orthogonal. Furthermore, $\sum_{j=1}^{k} \dim(S_j) = n$, which can be seen by noting that otherwise we could find some state orthogonal to every member of $\mathcal{U}$ on Bob's system, which violates unextendibility. Since each of P_j and Q_j contain sets of vectors that span S_j on Bob's system, it follows that $|\mathcal{U}| = \sum_{j=1}^{k} |P_j| + \sum_{j=1}^{k} |Q_j| \geq 2\sum_{j=1}^{k} \dim(S_j) = 2n$, which completes the proof. □

It follows from Theorem 2.2.2 that UPBs cannot be used to create PPT entangled states in $M_2 \otimes M_n$ (even though PPT entangled states exist in this space when $n \geq 4$).

2.2.2 Multipartite UPBs

We now introduce our first UPB in the multipartite setting. Consider the following set of four states in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\mathcal{U}_{\text{shifts}} \stackrel{\text{def}}{=} \Big\{ |0\rangle|0\rangle|0\rangle, |1\rangle|+\rangle|-\rangle, |-\rangle|1\rangle|+\rangle, |+\rangle|-\rangle|1\rangle \Big\}, \tag{2.5}$$

where we recall that $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. It is straightforward to verify that the members of $\mathcal{U}_{\text{shifts}}$ are mutually orthogonal, so we focus only on showing that this set is unextendible.

To see unextendibility, suppose that there were some product state $|z\rangle = |z^1\rangle \otimes |z^2\rangle \otimes |z^3\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ such that $\langle v|z\rangle = 0$ for all $|v\rangle \in \mathcal{U}_{\text{shifts}}$. Well, it is the case that $|z^1\rangle$ can be orthogonal to at most one of $|0\rangle, |1\rangle, |+\rangle$, or $|-\rangle$ (and similarly for $|z^2\rangle, |z^3\rangle$). Thus $|z^1\rangle \otimes |z^2\rangle \otimes |z^3\rangle$ can be orthogonal to at most $1+1+1 = 3$ members of $\mathcal{U}_{\text{shifts}}$, so no product state is orthogonal to all 4 members of $\mathcal{U}_{\text{shifts}}$.

Even though we only explicitly proved Proposition 2.2.1 in the bipartite case, an almost identical proof works for the general multipartite case as well, so we conclude that the state

$$\rho_{\text{shifts}} := \frac{1}{4}(I - \sum_{|v\rangle \in \mathcal{U}_{\text{shifts}}} |v\rangle\langle v|)$$

is entangled and PPT (i.e., applying the transpose map to any subset of the systems results in a positive semidefinite operator).

Multipartite Separability is Funky

We can use Theorem 2.2.2 to show that the state $\rho_{\text{shifts}} \in M_2 \otimes M_2 \otimes M_2$ is not only PPT across every bipartite cut, but it is even separable across every bipartite cut (even though it is not separable). To see this, we show that it is separable across the cut $M_2 \otimes (M_2 \otimes M_2) \cong M_2 \otimes M_4$ and simply note that the argument for the other cuts is almost identical.

Consider the product basis $\mathcal{U}_{\text{shifts}}$ as a subset of $\mathbb{C}^2 \otimes \mathbb{C}^4$ rather than $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ and notice that Theorem 2.2.2 says that it is extendible in this space (even though it is not extendible in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$). That is, we can find a product state $|v_5\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^4$ that is orthogonal to every member of $\mathcal{U}_{\text{shifts}}$. Similarly, since the set $\mathcal{U}_{\text{shifts}} \cup \{|v_5\rangle\}$ has only 5 members, we can use Theorem 2.2.2 again to find a product state $|v_6\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^4$ that is orthogonal to $|v_5\rangle$ as well as every member of $\mathcal{U}_{\text{shifts}}$. Continuing in this way, we can also find product states $|v_7\rangle, |v_8\rangle$ such that the set $\mathcal{U}_{\text{shifts}} \cup \{|v_5\rangle, |v_6\rangle, |v_7\rangle, |v_8\rangle\}$ is a complete orthonormal product basis of $\mathbb{C}^2 \otimes \mathbb{C}^4$.

It is then straightforward to verify that

$$\rho_{\text{shifts}} := \frac{1}{4}\Big(I - \sum_{|v\rangle \in \mathcal{U}_{\text{shifts}}} |v\rangle\langle v|\Big) = \frac{1}{4}\sum_{j=5}^{8} |v_j\rangle\langle v_j|,$$

which is separable in $M_2 \otimes M_4$ since each of the $|v_j\rangle$'s is a product state in $\mathbb{C}^2 \otimes \mathbb{C}^4$.

This example shows us that we cannot completely naïvely apply bipartite separability criteria and hope to characterize multipartite separability—a state can be separable across every bipartition without actually being separable!

Exercises

Exercise 2. Let $\mathcal{U} \subset \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots \otimes \mathbb{C}^{n_p}$ be an unextendible product basis with s members. Show that

$$s \geq \sum_{i=1}^{p} (n_i - 1) + 1.$$

Exercise 3. We showed in Section 2.2.2 that the state $\rho_{\text{shifts}} \in M_2 \otimes M_2 \otimes M_2$ is separable with respect to any bipartition. Find an explicit separable decomposition of ρ_{shifts} with respect to the bipartition $M_2 \otimes (M_2 \otimes M_2) \cong$

$M_2 \otimes M_4$. That is, find separable pure states $\{|v_i\rangle\} \subset \mathbb{C}^2 \otimes \mathbb{C}^4$ and positive scalars $\{p_i\}$ such that

$$\rho_{\text{shifts}} = \sum_{i=1}^{k} p_i |v_i\rangle\langle v_i|.$$

Lecture 3

Detecting PPT Entangled States: Realignment and Local Filters

We have already seen one method for detecting the entanglement in PPT states: the Choi map Φ_C. For example, it is straightforward to check that the following state $\rho = M_3 \otimes M_3$ is PPT:

$$\rho := \frac{1}{21}\begin{bmatrix} 2 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 2 \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 2 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & \cdot \\ 2 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 2 \end{bmatrix}, \tag{3.1}$$

yet $(id_3 \otimes \Phi_C)(\rho)$ has $-1/42$ as one of its eigenvalues. Since we know that Φ_C is positive (recall Theorem 1.2.6), this implies that ρ is entangled.

However, the state above is extremely "cooked up", and we can't expect the Choi map to save us like this in general. For example, the Choi map is unable to detect the entanglement in the ρ_{tiles} state based on the "tiles"

UPB (introduced in Section 2.2.1). So how can we detect entanglement in PPT states in practice?

3.1 The Realignment Criterion

Remember the Schmidt decomposition theorem for pure states? Well, there is an analogous theorem for mixed states (and even for arbitrary operators).

Theorem 3.1.1 (Operator Schmidt decomposition)**.** *For any matrix $X \in M_n \otimes M_m$ there exists an integer $1 \leq r \leq \min\{n^2, m^2\}$, strictly positive real scalars $\{\gamma_i\}_{i=1}^r$ with $\sum_{i=1}^r \gamma_i^2 = 1$, and orthonormal (in the Hilbert–Schmidt inner product) sets of matrices $\{A_i\}_{i=1}^r \subset M_n$ and $\{B_i\}_{i=1}^r \subset M_m$ such that*

$$X = \sum_{i=1}^r \gamma_i A_i \otimes B_i.$$

Furthermore, if X is Hermitian then the matrices $\{A_i\}$ and $\{B_i\}$ can be chosen to be Hermitian.

Proof. Almost identical to the proof of the Schmidt decomposition (just reshape the matrices into vectors and then back again). □

We note that this decomposition, just like the regular Schmidt decomposition, is easy to compute in practice, and can tell us a great deal about the entanglement of ρ. The main result of this section shows that the operator Schmidt decomposition can be used to detect entanglement in some quantum states.

Theorem 3.1.2 (Realignment criterion)**.** *Let $\rho \in M_n \otimes M_m$ have operator Schmidt decomposition*

$$\rho = \sum_{i=1}^r \gamma_i A_i \otimes B_i.$$

If $\sum_{i=1}^r \gamma_i > 1$ then ρ is entangled.

Proof. We prove the result by constructing an entanglement witness W that detects entanglement in ρ. In particular, we define

$$W := I - \sum_{i=1}^r A_i \otimes B_i.$$

We can see that $\mathrm{Tr}(W\rho) < 0$ as follows:

$$\begin{aligned}\mathrm{Tr}(W\rho) &= \mathrm{Tr}(\rho) - \mathrm{Tr}(\sum_{i,j=1}^{r} \gamma_j A_i A_j \otimes B_i B_j) \\ &= 1 - \sum_{i,j=1}^{r} \delta_{i,j}\gamma_j \\ &= 1 - \sum_{j=1}^{r} \gamma_j \\ &< 0,\end{aligned}$$

where we used the fact that the operators $\{A_i\}_{i=1}^r$ and $\{B_i\}_{i=1}^r$ are Hermitian and mutually orthonormal. It follows that *if* W is an entanglement witness then it detects entanglement in ρ.

To see that W is an entanglement witness, we need to show that its inner product with separable states is nonnegative:

$$\begin{aligned}(\langle a| \otimes \langle b|)W(|a\rangle \otimes |b\rangle) &= (\langle a| \otimes \langle b|)\Big(I - \sum_{i=1}^{r} A_i \otimes B_i\Big)(|a\rangle \otimes |b\rangle) \\ &= 1 - \sum_{i=1}^{r}\langle a|A_i|a\rangle\langle b|B_i|b\rangle.\end{aligned} \tag{3.2}$$

Now we define two vectors $\mathbf{a} \in \mathbb{R}^n$ and $\mathbf{b} \in \mathbb{R}^m$ by $\mathbf{a}_i := \langle a|A_i|a\rangle$ and $\mathbf{b}_i := \langle b|B_i|b\rangle$ (where we have extended $\{A_i\}$ and $\{B_i\}$ to full orthonormal bases of M_n and M_m, respectively). Since $\{A_i\}$ and $\{B_i\}$ form orthonormal bases of M_n and M_m, respectively, we know that $|a\rangle\langle a| = \sum_{i=1}^{n^2} \mathbf{a}_i A_i$ and $|b\rangle\langle b| = \sum_{i=1}^{m^2} \mathbf{b}_i B_i$. Thus

$$1 = \big\| |a\rangle\langle a| \big\|_F^2 = \Big\| \sum_{i=1}^{n^2} \mathbf{a}_i A_i \Big\|_F^2 = \sum_{i=1}^{n^2} |\mathbf{a}_i|^2 = \|\mathbf{a}\|^2,$$

where $\|\cdot\|_F$ is the Frobenius norm (i.e., the norm induced by the Hilbert–Schmidt inner product), and similarly for $\mathbf{b}$. It follows that

$$\sum_{i=1}^{r}\langle a|A_i|a\rangle\langle b|B_i|b\rangle = \sum_{i=1}^{r} \mathbf{a}_i\mathbf{b}_i \leq \|\mathbf{a}\|\|\mathbf{b}\| = 1,$$

where the inequality is the Cauchy–Schwarz inequality. This shows that (3.2) is nonnegative, which completes the proof. □

We claimed that the realignment criterion detects entanglement in some states that the PPT criterion cannot. To see that this is the case, consider the state ρ given by (3.1). It can be checked that this state has $\sum_{i=1}^{r} \gamma_i = \frac{1}{21}(19+2\sqrt{7}) > 1$, so Theorem 3.1.2 detects its entanglement even though it is PPT. Similarly, the state ρ_{tiles} has $\sum_{i=1}^{r} \gamma_i \approx 1.0874\ldots$, so the realignment criterion detects entanglement in that state as well.

Side note: The realignment criterion actually has several different forms and goes by two different names. The term “realignment criterion” comes from the fact that the coefficients $\{\gamma_i\}$ in the operator Schmidt decomposition are the singular values of a certain “realigned” matrix that results from shifting the entries of ρ around in the standard basis. Thus, computing $\sum_i \gamma_i$ is the same as computing the trace norm of this realigned matrix. This separability criterion is also sometimes called the *computable cross norm (CCN) criterion*. The reason for these different formulations of the same criterion is simply that it was introduced independently at the same time by different authors in two very different settings [CW03, Rud03].

3.2 Local Filters

We now introduce a general method for “boosting” the effectiveness of a separability criterion. The idea is to let $F_1 \in M_n$ and $F_2 \in M_m$ be invertible, and consider the transformation

$$\rho \mapsto \rho' := \frac{(F_1 \otimes F_2)\rho(F_1 \otimes F_2)^\dagger}{\mathrm{Tr}\Big((F_1 \otimes F_2)\rho(F_1 \otimes F_2)^\dagger\Big)}. \tag{3.3}$$

Transformations of this kind are called *local filters*. It is straightforward to show that ρ' is separable whenever ρ is separable. Furthermore, invertibility of F_1 and F_2 ensures that we can reverse this transformation, so we actually know that ρ' is separable *if and only if* ρ is separable.

Thus even if a particular separability criterion is unable to detect entanglement in ρ, there may yet be hope: we could try to find F_1 and F_2 such that the separability criterion detects entanglement in ρ' instead. For example, the proof of the following result makes use of local filters and the reduction map.

Proposition 3.2.1. *Let $\rho \in M_n \otimes M_m$ be separable. Then* $\mathrm{rank}(\rho) \geq \max\{\mathrm{rank}(\rho_A), \mathrm{rank}(\rho_B)\}$.

Proof. We only show that $\mathrm{rank}(\rho) \geq \mathrm{rank}(\rho_A)$, since the corresponding inequality for ρ_B is proved analogously. Also, we prove the contrapositive of the statement, so we start by assuming that $\mathrm{rank}(\rho) < \mathrm{rank}(\rho_A)$, and we prove that ρ is entangled.

First, we apply a particular local filter to ρ. If ρ_A has spectral decomposition $\rho_A = UDU^\dagger$, where U is unitary and D is diagonal, then we define $F_1 := UD^{-1/2}U^\dagger$, where $D^{-1/2}$ is the diagonal matrix whose (i,i)-entry is $1/\sqrt{d_{i,i}}$ if $d_{i,i} \neq 0$, and whose (i,i)-entry is 1 if $d_{i,i} = 0$. Then we investigate the separability of the filtered state

$$\rho' := \frac{(F_1 \otimes I)\rho(F_1 \otimes I)^\dagger}{\mathrm{Tr}\big((F_1 \otimes I)\rho(F_1 \otimes I)^\dagger\big)}.$$

Our reason for doing this is that

$$\rho'_A = \frac{\mathrm{Tr}_B\big((F_1 \otimes I)\rho(F_1 \otimes I)^\dagger\big)}{\mathrm{Tr}\big((F_1 \otimes I)\rho(F_1 \otimes I)^\dagger\big)} = \frac{F_1\rho_A F_1^\dagger}{\mathrm{Tr}(F_1\rho_A F_1^\dagger)} = P_A/\mathrm{rank}(\rho_A),$$

where P_A is the orthogonal projection onto the range of ρ_A. We now apply the reduction map R (from Section 1.2.2) to one half of ρ':

$$(id \otimes R)(\rho') = \mathrm{Tr}_B(\rho') \otimes I - \rho' = \rho'_A \otimes I - \rho' = (P_A \otimes I)/\mathrm{rank}(\rho_A) - \rho'.$$

Now let $|v\rangle$ be an eigenvector of ρ' corresponding to its maximal eigenvalue $\lambda_{\max}$. Since $\mathrm{Tr}(\rho') = 1$, it must be the case that $\lambda_{\max} \geq 1/\mathrm{rank}(\rho') = 1/\mathrm{rank}(\rho)$. Thus

$$\begin{aligned}\langle v|(id \otimes R)(\rho')|v\rangle &= \langle v|\big((P_A \otimes I)/\mathrm{rank}(\rho_A) - \rho'\big)|v\rangle \\ &\leq 1/\mathrm{rank}(\rho_A) - \langle v|\rho'|v\rangle \\ &\leq 1/\mathrm{rank}(\rho_A) - 1/\mathrm{rank}(\rho).\end{aligned} \tag{3.4}$$

Now we can use the fact that $\mathrm{rank}(\rho) < \mathrm{rank}(\rho_A)$ to conclude that the quantity (3.4) is strictly negative, so $(id \otimes R)(\rho') \not\geq 0$. It follows from the fact that the reduction map is positive that ρ is entangled. □

3.2.1 The Filter Normal Form

The idea presented in the proof of Proposition 3.2.1 actually applies in a fair bit of generality: one local filter that often helps us prove that a state is entangled is one that sends one of the reduced states of ρ to a scalar multiple of the identity matrix (i.e., the maximally-mixed state). In a sense, such a local filter is throwing away the irrelevant local information on one of the systems, leaving us only with local information on the other system as well as information about the entanglement between the systems.

The following theorem shows that it is often possible to find a local filter that even makes *both* of the reduced states maximally-mixed.

Theorem 3.2.2. *Suppose $\rho \in M_n \otimes M_m$ has full rank. Then there exist invertible $F_1 \in M_n$ and $F_2 \in M_m$ such that the locally filtered state ρ' described by (3.3) has operator Schmidt decomposition*

$$\rho' = \frac{1}{nm}\Big(I + \sum_{i=1}^{r} \xi_i G_i \otimes H_i\Big), \tag{3.5}$$

where each G_i and H_i is Hermitian and traceless.

Before proving this result, we note that the decomposition (3.5) is sometimes called the *filter normal form* of ρ. This form is useful because the corresponding filter can be thought of as the one that makes ρ the "most entangled" (even though we haven't actually changed whether ρ is separable or entangled). Thus if a separability criterion is not able to detect the entanglement in ρ, it might be a good idea to first convert ρ into its filter normal form and *then* apply the separability criterion.

Proof. For each state $\rho \in M_n \otimes M_m$, start by defining a function f_ρ that acts on $SL(n,\mathbb{C}) \times SL(m,\mathbb{C})$, the set of pairs of determinant-1 operators of the form $F_1 \in M_n$ and $F_2 \in M_m$, as follows:

$$f_\rho(F_1, F_2) := \mathrm{Tr}((F_1 \otimes F_2)\rho(F_1 \otimes F_2)^\dagger).$$

Our first goal is to minimize f_ρ, since it turns out that doing this will essentially tell us what local filter to use.

We will minimize f_ρ via an iterative procedure. Begin by setting $F_1 = \det(\rho_A)^{1/2n}\rho_A^{-1/2}$ and $F_2 = I$. Then

$$\begin{aligned} f_\rho(F_1, I) &= \mathrm{Tr}((F_1 \otimes I)\rho(F_1 \otimes I)^\dagger) = \mathrm{Tr}(F_1\rho_A F_1^\dagger) \\ &= \det(\rho_A)^{1/n}\mathrm{Tr}(I) = n\det(\rho_A)^{1/n} \leq 1 = f_\rho(I, I), \end{aligned} \tag{3.6}$$

where the final inequality comes from the arithmetic-geometric mean inequality applied to the eigenvalues of ρ_A. Furthermore, the arithmetic-geometric mean inequality tells us that equality holds in (3.6) if and only if $\rho_A = I/n$.

Now we set $\tilde{\rho} := (F_1 \otimes I)\rho(F_1 \otimes I)^\dagger / \mathrm{Tr}((F_1 \otimes I)\rho(F_1 \otimes I)^\dagger)$ and repeat this argument (but on Bob's system). Specifically, if we define $F_2 = \det(\tilde{\rho}_B)^{1/2n}\tilde{\rho}_B^{-1/2}$ then reasoning similar to that above shows that $f_{\tilde{\rho}}(I, F_2) = f_\rho(F_1, F_2) \leq f_\rho(F_1, I)$. Furthermore, equality holds if and only if $\tilde{\rho}_B = I_m$, just like before.

We now return to Alice's system and repeat this procedure, then back to Bob's, and so on ad infinitum. Since every step of this procedure reduces the value of f_ρ, and this function is clearly bounded below by 0, we must converge to a local minimum, which is attained by some particular $F_1 \otimes F_2$ (furthermore, this local minimum does not *equal* 0 since ρ has full rank and we are choosing F_1 and F_2 at each step to have determinant 1). Furthermore, the only stationary points of this procedure are those with both partial traces of $\rho' := (F_1 \otimes F_2)\rho(F_1 \otimes F_2)^\dagger / \mathrm{Tr}((F_1 \otimes F_2)\rho(F_1 \otimes F_2)^\dagger)$ proportional to the identity, so we must converge to such a point.

In particular, what we have proved is that there exists a local filter $F_1 \otimes F_2$ such that ρ' has $\rho'_A = I/n$ and $\rho'_B = I/m$. This is the local filter that is desired in the statement of the theorem. To see that the operator Schmidt decomposition has the desired form, consider the operator Schmidt decomposition of $\rho' - I/(nm)$:

$$\rho' - I/(nm) = \sum_{i=1}^{r} \gamma_i A_i \otimes B_i.$$

Since $\mathrm{Tr}_B(\rho' - I/(nm)) = 0$, we have $\sum_{i=1}^{r} \gamma_i \mathrm{Tr}(B_i) A_i = 0$. Since the A_i's are linearly independent, it follows that $\gamma_i \mathrm{Tr}(B_i) = 0$ for all i. However, $\gamma_i > 0$, so $\mathrm{Tr}(B_i) = 0$ for all i. A similar argument shows that $\mathrm{Tr}(A_i) = 0$ for all i. Thus

$$\rho' = \frac{1}{nm}\Big(I + \sum_{i=1}^{r} \xi_i G_i \otimes H_i\Big),$$

where $\xi_i = nm\gamma_i$, $G_i = A_i$, and $H_i = B_i$ for all i. The fact that this is an operator Schmidt decomposition of ρ' follows from the fact that each G_i and H_i is traceless and thus orthogonal to I. □

We note that the iterative procedure to find the local filter discussed in the proof of Theorem 3.2.2 works very well in practice. Furthermore, under some mild assumptions (see [Gur03] for details), the iterations converge exponentially quickly to the local filter that we desire.

The Filter Covariance Matrix Criterion

We are finally in a position to prove one of the strongest entanglement criteria that can be implemented "trivially" by software such as MATLAB.

Theorem 3.2.3 (Filter covariance matrix criterion)**.** *Suppose $\rho \in M_n \otimes M_m$ is separable and has filter normal form as in* (3.5)*. Then $\sum_{i=1}^r \xi_i \leq nm - \sqrt{nm}$.*

Proof. Just apply the realignment criterion to the filter normal form of ρ. Since ρ is separable, the locally filtered state ρ' is also separable. Since we have the following as an operator Schmidt decomposition of ρ':

$$\rho' = \frac{1}{nm}\Big(I + \sum_{i=1}^r \xi_i G_i \otimes H_i\Big),$$

it follows from Theorem 3.1.2 (and rescaling each matrix in the above decomposition to have Frobenius norm 1) that

$$\frac{1}{\sqrt{nm}} + \sum_{i=1}^r \frac{\xi_i}{nm} \leq 1.$$

Rearranging this inequality yields $\sum_{i=1}^r \xi_i \leq nm - \sqrt{nm}$, as desired. □

While Theorem 3.2.3 is perhaps difficult to use analytically, it performs extremely well numerically and can realistically be used on states living in very large spaces (e.g., $n, m \approx 50$).

Exercises

Exercise 4. Show that Proposition 3.2.1 holds for all PPT states, not just separable states. That is, let $\rho \in M_n \otimes M_m$ and show that $(id \otimes T)(\rho) \geq 0$ implies $\text{rank}(\rho) \geq \max\{\text{rank}(\rho_A), \text{rank}(\rho_B)\}$.

Lecture 4

Detecting PPT Entangled States: Symmetric Extensions

In this lecture, we present the most powerful separability criterion that is currently known, which is based on the idea of extending a state to one acting on a larger Hilbert space. The upside of this test is that it is fantastically strong. The downside is that it is much more computationally-intensive than the tests that we looked at previously.

4.1 Symmetric Extensions

If we are given a separable state $\rho \in M_n \otimes M_m$ with separable decomposition

$$\rho = \sum_{i=1}^{k} p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|,$$

notice that we can "extend" ρ to a state living on the tripartite space $M_n \otimes M_m \otimes M_m$ in a natural way:

$$\tilde{\rho} := \sum_{i=1}^{k} p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i| \otimes |b_i\rangle\langle b_i|. \tag{4.1}$$

In particular, $\tilde{\rho}$ is a valid quantum state that satisfies $\mathrm{Tr}_2(\tilde{\rho}) = \mathrm{Tr}_3(\tilde{\rho}) = \rho$. In fact, there is nothing special about just adding one more copy of M_m:

we can similarly find extensions of ρ in $M_n \otimes M_m^{\otimes s}$ for any $s \geq 2$ of the form

$$\tilde{\rho} = \sum_{i=1}^{k} p_i |a_i\rangle\langle a_i| \otimes \underbrace{|b_i\rangle\langle b_i| \otimes \cdots \otimes |b_i\rangle\langle b_i|}_{s \text{ copies}}.$$

As before, $\tilde{\rho}$ is a valid quantum state, and upon tracing out any $s-1$ copies of M_m we are left with the state ρ. This leads us to the following definition.

Definition 4.1.1. Let $\rho \in M_n \otimes M_m$. We say that ρ has an *s-copy symmetric extension* if there exists a state $\tilde{\rho} \in M_n \otimes M_m^{\otimes s}$ such that

$$\mathrm{Tr}_{\bar{1},\bar{i}}(\tilde{\rho}) = \rho \quad \forall\, 2 \leq i \leq s+1,$$

where $\mathrm{Tr}_{\bar{1},\bar{i}}$ denotes the partial trace over all systems *except* for the first and i-th systems.

As we already noted, separable states have s-copy symmetric extensions for all $s \geq 2$. What's more interesting is the fact that separable state are the *only* states with this property [DPS04]. That is, if a state is entangled then there exists some $s \geq 2$ such that it does not have an s-copy symmetric extension. Thus, symmetric extensions provide a complete family of separability criteria – if we could find some way to determine whether or not a state has an s-copy symmetric extension, we could completely solve the separability problem.

4.1.1 Semidefinite Programming

Unfortunately, we don't have time to give a *proper* introduction to semidefinite programming, so we'll just skim the basics. For a much more thorough introduction, see [Wat11].

A *semidefinite program (SDP)* is a certain type of convex optimization problem that is useful both theoretically and numerically. For our purposes though, we won't get into its theoretical niceties, and will instead focus only on its excellent numerical properties. In particular, semidefinite programs can be solved efficiently—if you so desire, you can download the free CVX package [GB12] for MATLAB, which provides a simple interface for solving SDPs numerically.

First, a linear map $\Phi : M_n \to M_m$ is called *Hermiticity-preserving* if $\Phi(X)^\dagger = \Phi(X)$ whenever $X^\dagger = X$. Then a semidefinite program is an optimization problem defined by a Hermiticity-preserving linear map $\Phi : M_n \to M_m$ and two operators $A \in M_n$ and $B \in M_m$. The semidefinite program associated with Φ, A, and B is the following optimization problem:

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(AX) \\ \text{subject to:} \quad & \Phi(X) - B \geq 0 \\ & X \geq 0 \end{aligned} \tag{4.2}$$

In the above SDP, we optimize over positive semidefinite matrices $X \in M_n$, and the constraints of the form "≥ 0" mean that the matrices on the left are positive semidefinite. If "≥ 0" instead meant that each entry of the matrix were nonnegative (and all of the matrices considered were real), then this would be a *linear program*, which you may have learned about during your undergraduate studies.

As you might have guessed, semidefinite programming is exactly the tool that is used to determine whether or not a given state $\rho \in M_n \otimes M_m$ has an s-copy symmetric extension. In particular, the following SDP works in the $s = 2$ case:

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(X) \\ \text{subject to:} \quad & \mathrm{Tr}_2(X) = \rho \\ & \mathrm{Tr}_3(X) = \rho \\ & X \geq 0 \end{aligned} \tag{4.3}$$

where we optimize over positive semidefinite $X \in M_n \otimes M_m \otimes M_m$. Note that this optimization problem is not *quite* in the form (4.2), but it is hopefully at least somewhat believable that it could be massaged to be in that form. This SDP also generalizes to s-copy symmetric extensions in a straightforward manner.

Notice that if ρ has a 2-copy symmetric extension then the SDP (4.3) has optimal value 1, since every symmetric extension X of ρ has $\mathrm{Tr}(X) = \mathrm{Tr}(\rho) = 1$. On the other hand, if ρ does not have a 2-copy symmetric extension, then there is no X satisfying the constraints of the SDP (4.3). In this case, the SDP returns an optimal value of $+\infty$.

A few notes:

- Although semidefinite programs can be solved efficiently, determining whether or not a state has a s-copy symmetric extension is much slower than the methods discussed previously in this module, even when $s = 2$.

- Furthermore, symmetric extensions themselves do not provide a very strong test for entanglement (as we will see in the next section). However...
- We can augment this test by searching for a symmetric extension that also satisfies another separability criterion, such as the PPT criterion or the realignment criterion. The PPT criterion is almost always what is used in practice.

To illustrate what we mean by the third point above, consider the following variant of the SDP (4.3):

$$\begin{array}{rl} \text{minimize:} & \mathrm{Tr}(X) \\ \text{subject to:} & \mathrm{Tr}_2(X) = \rho \\ & \mathrm{Tr}_3(X) = \rho \\ & (id \otimes id \otimes T)(X) \geq 0 \\ & X \geq 0 \end{array}$$

As you can see, this SDP determines whether or not ρ has a symmetric extension that also has positive partial transpose. This is a fine thing to search for, since we can see from (4.1) that every separable state has a symmetric extension that is not only PPT, but is even separable itself, so it passes any separability criteria we can throw at it. We could add in another constraint that requires that the symmetric extension has positive partial transpose when the transpose is applied to the first system instead of the third, or a transpose that is applied to any combination of the systems that we choose.

What we end up with is a trade-off game: the more constraints we add to the SDP, the longer the SDP will take to run, but the more effective it is. We could even add the realignment criterion as one of the constraints (but this is more complicated) or first apply a local filter to ρ before running the SDP.

4.2 Comparison of Methods

We have seen many methods for detecting entanglement in quantum states in this module, but we have not yet discussed their effectiveness too much. We now investigate how well these separability criteria work on one specific family of quantum states.

Separability criterion used	Maximal p detected
2-copy symmetric extension	none
3-copy symmetric extension	0.0309
4-copy symmetric extension	0.0445
realignment criterion (Theorem 3.1.2)	0.1103
filter covariance matrix criterion (Theorem 3.2.3)	0.1278
2-copy PPT symmetric extension	0.1351
3-copy PPT symmetric extension	0.1351
4-copy PPT symmetric extension	0.1351

Table 4.1: A comparison of the effectiveness of the various separability criteria that were introduced in this module. The column on the right gives the (approximate) largest value of p such that the given separability criterion is able to detect the entanglement in the state ρ_p. Larger values of p intuitively correspond to stronger separability criteria.

4.2.1 The Noisy "Tiles" State

Recall from Lecture 2 that we created an unextendible product basis $\mathcal{U}_{\text{tiles}}$ and then showed that it can be used to create a PPT entangled state $\rho_{\text{tiles}} \in M_3 \otimes M_3$ via Proposition 2.2.1. In order to really put our separability criteria to the test, consider the following state, which is a mixture of ρ_{tiles} and the maximally-mixed state $I/9$ that depends on a real parameter $0 \leq p \leq 1$:

$$\rho_p := pI/9 + (1-p)\rho_{\text{tiles}}.$$

When $p = 0$, $\rho_p = \rho_{\text{tiles}}$, which is entangled, and when $p = 1$, $\rho_p = I/9$, which is separable. By convexity of the set of separable states, we know that there exists some particular $p^* \in (0, 1]$ such that ρ_p is entangled whenever $p < p^*$ and ρ_p is separable whenever $p \geq p^*$. Intuitively, the entanglement in ρ_p becomes more difficult to detect as p increases.

As discussed in previous lectures, the partial transpose, reduction map, and Choi map are all incapable of detecting entanglement in ρ_{tiles}, so they are incapable of detecting entanglement in any ρ_p. Table 4.1 provides the (approximate) largest value of p such that a given entanglement test is able to detect entanglement in ρ_p.

As we see from the table, the tests based on symmetric extensions themselves seem to be fairly weak, but they then become even stronger than the filter covariance matrix criterion when used in conjunction with the PPT criterion. For what it's worth, we only know that ρ_p is separable when $p \geq 0.4367$. Thus there is a rather large gap of values $p \in (0.1351, 0.4367)$ where we do not know whether or not ρ_p is entangled.

Exercises

Exercise 5. Let $a \in (0, \infty)$ be a real number and define a quantum state $\rho_a \in M_3 \otimes M_3$ by its standard basis representation

$$\rho_a := \frac{a}{3(1+a+a^2)} \begin{bmatrix} 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & 1/a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1/a & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1/a & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \end{bmatrix}.$$

Notice that the $a = 2$ case gives the state (3.1).

a) Show that ρ_a has positive partial transpose for all $a \in (0, \infty)$.

b) Show that ρ_a is entangled for all $a \in (0, 1) \cup (1, \infty)$. You may use any entanglement test of your choosing.

Side note: It turns out that ρ_a is separable when $a = 1$.

Bibliography

[CW03] K. Chen and L.-A. Wu. A matrix realignment method for recognizing entanglement. *Quantum Inf. Comput.*, 3:193–202, 2003. 22

[DPS04] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. A complete family of separability criteria. *Phys. Rev. A*, 69:022308, 2004. 28

[GB12] Michael Grant and Stephen Boyd. CVX: MATLAB software for disciplined convex programming, version 2.0 beta. http://cvxr.com/cvx, September 2012. 28

[Gur03] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 10–19, 2003. 4, 26

[Rud03] O. Rudolph. Some properties of the computable cross norm criterion for separability. *Phys. Rev. A*, 67:032312, 2003. 22

[Stø63] E. Størmer. Positive linear maps of operator algebras. *Acta Math.*, 110:233–278, 1963. 5

[Wat11] J. Watrous. Theory of quantum information lecture notes, lecture 7. published electronically at http://www.cs.uwaterloo.ca/~watrous/lecture-notes.html, 2011. 28

[Wor76] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.*, 10:165–183, 1976. 5