Separability from Spectrum for Qubit–Qudit States

Nathaniel Johnston

CMS Winter Meeting 2013

December 8, 2013
We consider the separability problem in bipartite quantum systems:

**Question**

Given $X \in M_m \otimes M_n$, can we find positive semidefinite $\{P_i\} \subset M_m$ and $\{Q_i\} \subset M_n$ such that

$$X = \sum_i P_i \otimes Q_i?$$

If $X$ can be decomposed in this way, it is called **separable**. Otherwise, it is **entangled**.
We consider the separability problem in bipartite quantum systems:

**Question**

Given $X \in M_m \otimes M_n$, can we find positive semidefinite $\{ P_i \} \subset M_m$ and $\{ Q_i \} \subset M_n$ such that

\[ X = \sum_i P_i \otimes Q_i. \]

If $X$ can be decomposed in this way, it is called **separable**. Otherwise, it is **entangled**.
We consider the separability problem in bipartite quantum systems:

**Question**

Given $X \in M_m \otimes M_n$, can we find positive semidefinite $\{P_i\} \subset M_m$ and $\{Q_i\} \subset M_n$ such that

$$X = \sum_i P_i \otimes Q_i?$$

If $X$ can be decomposed in this way, it is called **separable**. Otherwise, it is **entangled**.
Entangled states are, in some senses, those that are “useful” in quantum computing:

- Well-known protocols such as superdense coding or quantum teleportation require entanglement;
- All entangled states can be used to improve quantum channel discrimination;
- Etc.

We thus would like simple methods for showing that certain states are separable or entangled.
Entangled states are, in some senses, those that are “useful” in quantum computing:

- Well-known protocols such as superdense coding or quantum teleportation require entanglement;
- All entangled states can be used to improve quantum channel discrimination;
- Etc.

We thus would like simple methods for showing that certain states are separable or entangled.
Entangled states are, in some senses, those that are “useful” in quantum computing:

- Well-known protocols such as superdense coding or quantum teleportation require entanglement;
- All entangled states can be used to improve quantum channel discrimination;
- Etc.

We thus would like simple methods for showing that certain states are separable or entangled.
Entangled states are, in some senses, those that are “useful” in quantum computing:

- Well-known protocols such as superdense coding or quantum teleportation require entanglement;
- All entangled states can be used to improve quantum channel discrimination;
- Etc.

We thus would like simple methods for showing that certain states are separable or entangled.
Entangled states are, in some senses, those that are “useful” in quantum computing:

- Well-known protocols such as superdense coding or quantum teleportation require entanglement;
- All entangled states can be used to improve quantum channel discrimination;
- Etc.

We thus would like simple methods for showing that certain states are separable or entangled.
One of the simplest methods for testing separability is based on the transpose map.

**Definition**

The partial transpose map $\Gamma : M_m \otimes M_n \rightarrow M_m \otimes M_n$ is defined by

$$\Gamma(A \otimes B) = A \otimes B^T,$$

where $T$ is the usual matrix transpose.

Matrices $X \in M_m \otimes M_n$ for which $\Gamma(X)$ is positive semidefinite are said to have **positive partial transpose (PPT)**.
One of the simplest methods for testing separability is based on the transpose map.

Definition

The **partial transpose** map \( \Gamma : M_m \otimes M_n \to M_m \otimes M_n \) is defined by

\[
\Gamma(A \otimes B) = A \otimes B^T,
\]

where \( T \) is the usual matrix transpose.

Matrices \( X \in M_m \otimes M_n \) for which \( \Gamma(X) \) is positive semidefinite are said to have **positive partial transpose (PPT)**.
One of the simplest methods for testing separability is based on the transpose map.

**Definition**

The *partial transpose* map \( \Gamma : M_m \otimes M_n \rightarrow M_m \otimes M_n \) is defined by

\[
\Gamma(A \otimes B) = A \otimes B^T,
\]

where \( T \) is the usual matrix transpose.

Matrices \( X \in M_m \otimes M_n \) for which \( \Gamma(X) \) is positive semidefinite are said to have **positive partial transpose (PPT)**.
Positive Partial Transpose

**Theorem**

*If* \( X \in M_m \otimes M_n \) *is separable then it has positive partial transpose.*

**Proof:** Since \( X \) is separable, we can write \( X = \sum_i P_i \otimes Q_i \). Then \( \Gamma(X) = \sum_i P_i \otimes Q_i^T \). Since each \( P_i \) and \( Q_i^T \) is positive semidefinite, so is \( \Gamma(X) \).

This gives a simple way to prove that a given operator is entangled.
Theorem

If $X \in M_m \otimes M_n$ is separable then it has positive partial transpose.

Proof: Since $X$ is separable, we can write $X = \sum_i P_i \otimes Q_i$. Then $\Gamma(X) = \sum_i P_i \otimes Q_i^T$. Since each $P_i$ and $Q_i^T$ is positive semidefinite, so is $\Gamma(X)$.

This gives a simple way to prove that a given operator is entangled.
Theorem

If \( X \in M_m \otimes M_n \) is separable then it has positive partial transpose.

**Proof:** Since \( X \) is separable, we can write \( X = \sum_i P_i \otimes Q_i \). Then \( \Gamma(X) = \sum_i P_i \otimes Q_i^T \). Since each \( P_i \) and \( Q_i^T \) is positive semidefinite, so is \( \Gamma(X) \).

This gives a simple way to prove that a given operator is entangled.
Remarkably, the converse is true when $m = 2$ and $n \leq 3$.

That is, if $X \in M_2 \otimes M_3$ has positive partial transpose then $X$ is separable.

This implication fails in all larger dimensions (i.e., when $m, n \geq 3$ and when $m = 2, n \geq 4$).

So how can we prove that a given operator is separable in larger dimensions?
Remarkably, the converse is true when $m = 2$ and $n \leq 3$.

That is, if $X \in M_2 \otimes M_3$ has positive partial transpose then $X$ is separable.

This implication fails in all larger dimensions (i.e., when $m, n \geq 3$ and when $m = 2$, $n \geq 4$).

So how can we prove that a given operator is separable in larger dimensions?
Remarkably, the converse is true when $m = 2$ and $n \leq 3$.

That is, if $X \in M_2 \otimes M_3$ has positive partial transpose then $X$ is separable.

This implication fails in all larger dimensions (i.e., when $m, n \geq 3$ and when $m = 2, n \geq 4$).

So how can we prove that a given operator is separable in larger dimensions?
Remarkably, the converse is true when $m = 2$ and $n \leq 3$.

That is, if $X \in M_2 \otimes M_3$ has positive partial transpose then $X$ is separable.

This implication fails in all larger dimensions (i.e., when $m, n \geq 3$ and when $m = 2, n \geq 4$).

So how can we prove that a given operator is separable in larger dimensions?
Balls of Separability

Any state that is sufficiently close to the identity matrix $I_m \otimes I_n$ is necessarily separable:

**Theorem (Gurvits–Barnum, 2002)**

If $X = X^\dagger \in M_m \otimes M_n$ satisfies $\|X - I_m \otimes I_n\|_F \leq 1$ then $X$ is separable, where $\| \cdot \|_F$ is the Frobenius norm.

In other words, there is a “ball of separability” centered at the identity operator.
Balls of Separability

Any state that is sufficiently close to the identity matrix $I_m \otimes I_n$ is necessarily separable:

**Theorem (Gurvits–Barnum, 2002)**

If $X = X^\dagger \in M_m \otimes M_n$ satisfies $\|X - I_m \otimes I_n\|_F \leq 1$ then $X$ is separable, where $\| \cdot \|_F$ is the Frobenius norm.

In other words, there is a “ball of separability” centered at the identity operator.
Any state that is sufficiently close to the identity matrix $I_m \otimes I_n$ is necessarily separable:

**Theorem (Gurvits–Barnum, 2002)**

If $X = X^\dagger \in M_m \otimes M_n$ satisfies $\|X - I_m \otimes I_n\|_F \leq 1$ then $X$ is separable, where $\| \cdot \|_F$ is the Frobenius norm.

In other words, there is a “ball of separability” centered at the identity operator.
The ball of separability depends only on the eigenvalues of $X$:

$$\|X - I_m \otimes I_n\|_F \leq 1 \text{ if and only if } \sum_i (\lambda_i - 1)^2 \leq 1,$$

where $\{\lambda_i\}$ are the eigenvalues of $X$.

Can we do better than this? Can we prove separability of even more matrices based only on their eigenvalues?
The ball of separability depends only on the eigenvalues of $X$:

$$\|X - I_m \otimes I_n\|_F \leq 1 \text{ if and only if } \sum_i (\lambda_i - 1)^2 \leq 1,$$

where $\{\lambda_i\}$ are the eigenvalues of $X$.

Can we do better than this? Can we prove separability of even more matrices based only on their eigenvalues?
Definition

A matrix $X = X^\dagger \in M_m \otimes M_n$ is called \textit{separable from spectrum} if all matrices $Y = Y^\dagger \in M_m \otimes M_n$ with the same eigenvalues as $X$ are separable.

All states in the ball of separability are separable from spectrum. But there are more!
A matrix $X = X^\dagger \in M_m \otimes M_n$ is called **separable from spectrum** if all matrices $Y = Y^\dagger \in M_m \otimes M_n$ with the same eigenvalues as $X$ are separable.

All states in the ball of separability are separable from spectrum. But there are more!
The two-qubit case had already been solved completely when the ball of separability was found:

**Theorem (Verstraete–Audenaert–Moor, 2001)**

A matrix $X \in M_2 \otimes M_2$ is separable from spectrum if and only if its eigenvalues $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4 \geq 0$ satisfy

$$\lambda_1 \leq \lambda_3 + 2\sqrt{\lambda_2 \lambda_4}.$$
The two-qubit case had already been solved completely when the ball of separability was found:

**Theorem (Verstraete–Audenaert–Moor, 2001)**

A matrix $X \in M_2 \otimes M_2$ is separable from spectrum if and only if its eigenvalues $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4 \geq 0$ satisfy

$$\lambda_1 \leq \lambda_3 + 2\sqrt{\lambda_2 \lambda_4}.$$
The two-qubit case had already been solved completely when the ball of separability was found:

**Theorem (Verstraete–Audenaert–Moor, 2001)**

A matrix $X \in M_2 \otimes M_2$ is separable from spectrum if and only if its eigenvalues $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4 \geq 0$ satisfy

$$\lambda_1 \leq \lambda_3 + 2\sqrt{\lambda_2 \lambda_4}.$$  

What about in higher-dimensional systems?
The idea: simplify things by replacing “separable” by “positive partial transpose”.

**Definition**

A matrix $X = X^\dagger \in M_m \otimes M_n$ is called PPT from spectrum if all matrices $Y = Y^\dagger \in M_m \otimes M_n$ with the same eigenvalues as $X$ have positive partial transpose.

(Hildebrand, 2007) completely solved the PPT from spectrum problem in all dimensions.
The idea: simplify things by replacing “separable” by “positive partial transpose”.

**Definition**

A matrix $X = X^\dagger \in M_m \otimes M_n$ is called **PPT from spectrum** if all matrices $Y = Y^\dagger \in M_m \otimes M_n$ with the same eigenvalues as $X$ have positive partial transpose.

(Hildebrand, 2007) completely solved the PPT from spectrum problem in all dimensions.
The idea: simplify things by replacing “separable” by “positive partial transpose”.

**Definition**

A matrix \( X = X^\dagger \in M_m \otimes M_n \) is called PPT from spectrum if all matrices \( Y = Y^\dagger \in M_m \otimes M_n \) with the same eigenvalues as \( X \) have positive partial transpose.

(Hildebrand, 2007) completely solved the PPT from spectrum problem in all dimensions.
The solution in arbitrary dimensions is a bit complicated, but it’s very simple in the qubit–qudit case (i.e., when \( m = 2 \) and \( n \) is arbitrary).

**Theorem (Hildebrand, 2007)**

A matrix \( X = X^\dagger \in M_2 \otimes M_n \) is PPT from spectrum if and only if its eigenvalues \( \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{2n} \geq 0 \) satisfy

\[
\lambda_1 \leq \lambda_{2n-1} + 2\sqrt{\lambda_{2n-2}\lambda_{2n}}.
\]

Since separability and PPT coincide when \( m = 2, n \leq 3 \), this immediately implies that \( X \in M_2 \otimes M_3 \) is separable from spectrum if and only if \( \lambda_1 \leq \lambda_5 + 2\sqrt{\lambda_4\lambda_6} \).
The solution in arbitrary dimensions is a bit complicated, but it’s very simple in the qubit–qudit case (i.e., when \( m = 2 \) and \( n \) is arbitrary).

**Theorem (Hildebrand, 2007)**

A matrix \( X = X^\dagger \in M_2 \otimes M_n \) is PPT from spectrum if and only if its eigenvalues \( \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{2n} \geq 0 \) satisfy

\[
\lambda_1 \leq \lambda_{2n-1} + 2\sqrt{\lambda_{2n-2}\lambda_{2n}}.
\]

Since separability and PPT coincide when \( m = 2, n \leq 3 \), this immediately implies that \( X \in M_2 \otimes M_3 \) is separable from spectrum if and only if \( \lambda_1 \leq \lambda_5 + 2\sqrt{\lambda_4\lambda_6} \).
The solution in arbitrary dimensions is a bit complicated, but it’s very simple in the qubit–qudit case (i.e., when \( m = 2 \) and \( n \) is arbitrary).

**Theorem (Hildebrand, 2007)**

A matrix \( X = X^\dagger \in M_2 \otimes M_n \) is PPT from spectrum if and only if its eigenvalues \( \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{2n} \geq 0 \) satisfy

\[
\lambda_1 \leq \lambda_{2n-1} + 2\sqrt{\lambda_{2n-2}\lambda_{2n}}.
\]

Since separability and PPT coincide when \( m = 2, n \leq 3 \), this immediately implies that \( X \in M_2 \otimes M_3 \) is separable from spectrum if and only if \( \lambda_1 \leq \lambda_5 + 2\sqrt{\lambda_4\lambda_6} \).
Our main result shows that PPT from spectrum and separability from spectrum coincide in $M_2 \otimes M_n$, regardless of $n$.

**Theorem**

Let $X = X^\dagger \in M_2 \otimes M_n$. Then $X$ is separable from spectrum if and only if it is PPT from spectrum.

Recall that the corresponding theorem fails for all $n \geq 4$ if we remove “from spectrum”.
Our main result shows that PPT from spectrum and separability from spectrum coincide in $M_2 \otimes M_n$, regardless of $n$.

**Theorem**

Let $X = X^\dagger \in M_2 \otimes M_n$. Then $X$ is separable from spectrum if and only if it is PPT from spectrum.

Recall that the corresponding theorem fails for all $n \geq 4$ if we remove “from spectrum”.
Our main result shows that PPT from spectrum and separability from spectrum coincide in $M_2 \otimes M_n$, regardless of $n$.

**Theorem**

Let $X = X^\dagger \in M_2 \otimes M_n$. Then $X$ is separable from spectrum if and only if it is PPT from spectrum.

Recall that the corresponding theorem fails for all $n \geq 4$ if we remove “from spectrum”.
Begin by writing $X \in M_2 \otimes M_n$ as a block matrix:

$$X = \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix}.$$ 

Intuitively, $X$ will be separable as long as $B$ is sufficiently “small” compared to $A$ and $C$. We can make this precise:

**Lemma**

If $\|B\|^2 \leq \lambda_{\min}(A) \cdot \lambda_{\min}(C)$ then $X$ is separable.
Sketch of Proof

Begin by writing $X \in M_2 \otimes M_n$ as a block matrix:

$$X = \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix}.$$  

Intuitively, $X$ will be separable as long as $B$ is sufficiently “small” compared to $A$ and $C$. We can make this precise:

**Lemma**

If $\|B\|^2 \leq \lambda_{\text{min}}(A) \cdot \lambda_{\text{min}}(C)$ then $X$ is separable.
Begin by writing $X \in M_2 \otimes M_n$ as a block matrix:

$$X = \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix}.$$

Intuitively, $X$ will be separable as long as $B$ is sufficiently “small” compared to $A$ and $C$. We can make this precise:

**Lemma**

If $\|B\|^2 \leq \lambda_{\min}(A) \cdot \lambda_{\min}(C)$ then $X$ is separable.
We would like to show that every PPT from spectrum $X$ satisfies the hypotheses of the previous lemma... but this is false!

So we instead prove that, for every PPT from spectrum $X$, there exists a unitary matrix $U \in M_2$ such that $(U \otimes I)^\dagger X(U \otimes I)$ satisfies the hypotheses of the lemma.

Thus $(U \otimes I)^\dagger X(U \otimes I)$ is separable, so $X$ is separable as well (and separability from spectrum then follows fairly quickly). □
We would like to show that every PPT from spectrum $X$ satisfies the hypotheses of the previous lemma... but this is false!

So we instead prove that, for every PPT from spectrum $X$, there exists a unitary matrix $U \in M_2$ such that $(U \otimes I)^\dagger X(U \otimes I)$ satisfies the hypotheses of the lemma.

Thus $(U \otimes I)^\dagger X(U \otimes I)$ is separable, so $X$ is separable as well (and separability from spectrum then follows fairly quickly). ■
We would like to show that every PPT from spectrum $X$ satisfies the hypotheses of the previous lemma... but this is false!

So we instead prove that, for every PPT from spectrum $X$, there exists a unitary matrix $U \in M_2$ such that $(U \otimes I)^\dagger X(U \otimes I)$ satisfies the hypotheses of the lemma.

Thus $(U \otimes I)^\dagger X(U \otimes I)$ is separable, so $X$ is separable as well (and separability from spectrum then follows fairly quickly). ■
We have shown that separability from spectrum is equivalent to PPT from spectrum when $m = 2$. What about when $m, n \geq 3$?

I don’t know.

I have plenty of evidence that PPT from spectrum and separability from spectrum coincide when $m = n = 3$, but still no proof.
We have shown that separability from spectrum is equivalent to PPT from spectrum when $m = 2$. What about when $m, n \geq 3$?

I don’t know.

I have plenty of evidence that PPT from spectrum and separability from spectrum coincide when $m = n = 3$, but still no proof.
We have shown that separability from spectrum is equivalent to PPT from spectrum when $m = 2$. What about when $m, n \geq 3$?

I don’t know.

I have plenty of evidence that PPT from spectrum and separability from spectrum coincide when $m = n = 3$, but still no proof.
Conjecture

Let $X = X^\dagger \in M_m \otimes M_n$. Then $X$ is separable from spectrum if and only if it is PPT from spectrum.

There is good “physics-y” intuition for believing this conjecture:

If it were false, then there would exist an entangled quantum state $X \in M_m \otimes M_n$ with the property that Alice and Bob cannot distill any pure entanglement from $X$, even if they are allowed to first apply arbitrary (non-local!!) quantum gates $U$ to $X$. 
Conjecture

Let $X = X^\dagger \in M_m \otimes M_n$. Then $X$ is separable from spectrum if and only if it is PPT from spectrum.

There is good “physics-y” intuition for believing this conjecture:

If it were false, then there would exist an entangled quantum state $X \in M_m \otimes M_n$ with the property that Alice and Bob can not distill any pure entanglement from $X$, even if they are allowed to first apply arbitrary (non-local!!) quantum gates $U$ to $X$. 
Thank-you!