Quantum State Local Distinguishability via Convex Optimization

PhD Defense

Alessandro Cosentino

University of Waterloo

August 13, 2015

Outline

State distinguishability problem

Cone programming framework

Applications
- Maximally entangled states
- Unextendable product sets

Conclusions

State distinguishability problem

Quantum state distinguishability problem

An instance of the problem is specified by an ensemble of N states

$$\{(p_1, \rho_1), \ldots, (p_N, \rho_N)\},$$

The problem

- An index $k \in \{1, \ldots, N\}$ is picked at random with prob. p_k
- The state ρ_k is prepared on a register X
- Alice is asked to identify k by means of measurements on X

Observations

- *Classical* states are always completely distinguishable
- *Orthogonal* quantum states are perfectly distinguishability

Quantum state *local* distinguishability problem

In the ensemble

$$\{(p_1, \rho_1), \ldots, (p_N, \rho_N)\},$$

the states $\rho_1, \ldots, \rho_N \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ are now bipartite states.

The problem

- An index $k \in \{1, \ldots, N\}$ is picked at random with prob. p_k
- The state ρ_k is prepared on a register X shared by two parties
- Alice and Bob are asked to identify k by Local Operations and Classical Communication (LOCC) on X

Motivations

- Understanding nonlocality/entanglement
- Applications to *secret sharing, data hiding, channel capacity*
- LOCC protocols are interesting from a physical point of view

Quantum state local distinguishability problem

Typical assumptions

- Sets of *orthogonal pure* states
- Perfect distinguishability (with probability 1)
- *Uniform* probability of selection ($p_1 = \cdots = p_N = 1/N$)

Distinguishable

- *any* 2 pure states
  [Walgate et al., '00]
- *any* 3 maximally entangled states in $\mathbb{C}^3 \otimes \mathbb{C}^3$
  [Nathanson - '05]
- ...

Indistinguishable

- *any* set of 3 or 4 Bell states
  [Ghosh et al, '01]
- 9 *product* states in $\mathbb{C}^3 \otimes \mathbb{C}^3$
  [Bennett et al. - PRA, 1999]
- ...

Quantum measurements and LOCC

N-outcome bipartite measurement

$$\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$$

$$\sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}}$$

LOCC measurements

- Difficult object to handle mathematically
- A cumbersome formal definition
- Many kinds of LOCC

$$\mathrm{LOCC}_1 \subsetneq \mathrm{LOCC}_r \subsetneq \mathrm{LOCC}_{r+1} \subsetneq \mathrm{LOCC}_{\mathrm{N}} \subsetneq \mathrm{LOCC} \subsetneq \overline{\mathrm{LOCC}} \subsetneq \mathrm{SEP} \subsetneq \mathrm{PPT}$$

(from Laura Mančinska's PhD thesis)

Separable and PPT measurements

Separable operators

$$P = \sum_{k=1}^{M} Q_k \otimes R_k \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y}), \qquad M > 0,\ Q_1, \ldots, Q_M \in \mathrm{Pos}(\mathcal{X}),\ R_1, \ldots, R_M \in \mathrm{Pos}(\mathcal{Y})$$

PPT (Positive-partial-transpose) operators

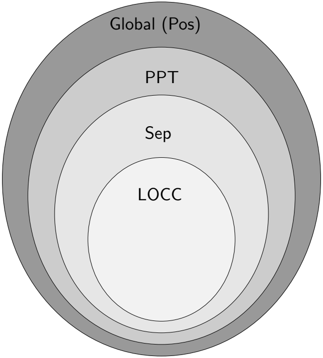
$$\mathrm{PPT}(\mathcal{X} : \mathcal{Y}) = \{P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \,:\, \mathsf{T}_{\mathcal{X}}(P) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})\}$$

Separable/PPT measurements

$\mu(k) \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$, or
$\mu(k) \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$

(for each $k \in \{1, \ldots, N\}$)

Classes of measurements



- A bound on PPT/Sep reflects into a bound on LOCC
- Optimizing over Sep is NP-hard
- Optimizing over PPT is computationally easy

Cone programming framework

Semidefinite program for global state distinguishability

- One of the first applications of SDP in quantum [Eldar, Megretski, Verghese, '03]

<u>Primal (Global)</u>

$$
\begin{aligned}
\text{max:} \quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\
\text{s.t.:} \quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}}, \\
& \mu : \{1, \ldots, N\} \rightarrow \mathrm{Pos}(\mathcal{X})
\end{aligned}
$$

<u>Dual (Global)</u>

$$
\begin{aligned}
\text{min:} \quad & \mathrm{Tr}(H) \\
\text{s.t.:} \quad & H - p_k \rho_k \in \mathrm{Pos}(\mathcal{X}) \\
& \qquad (k = 1, \ldots, N), \\
& H \in \mathrm{Herm}(\mathcal{X}).
\end{aligned}
$$

- *Weak duality*: any H feasible solution of the dual gives an upper bound on the optimal value of the primal

General cone program for bipartite state distinguishability

Primal

$$\text{max:} \quad \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle,$$

$$\text{s.t.:} \quad \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}},$$

$$\boxed{\mu : \{1, \ldots, N\} \to \mathcal{C}}$$

Dual

$$\text{min:} \quad \mathrm{Tr}(H)$$

$$\text{s.t.:} \quad \boxed{H - p_k \rho_k \in \mathcal{C}^*}$$

$$(k = 1, \ldots, N),$$

$$H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}).$$

- $\mathcal{C} \subseteq \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is a closed convex cone
- $\mathcal{C}^*$ is the cone dual to $\mathcal{C}$, that is,

$$\mathcal{C}^* = \{ Y \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}) \ : \ \langle X, Y \rangle \geq 0 \ \text{ for all } X \in \mathcal{C} \}$$

- $\mathrm{Pos}(\mathcal{X})$ is self-dual: $\mathrm{Pos}(\mathcal{X}) = (\mathrm{Pos}(\mathcal{X}))^*$

Cone program for PPT distinguishability

Primal (PPT)

$$\begin{aligned} \text{max:}\quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\ \text{s.t.:}\quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}}, \\ & \mu : \{1, \ldots, N\} \rightarrow \mathrm{PPT}(\mathcal{X} : \mathcal{Y}) \end{aligned}$$

Dual (PPT)

$$\begin{aligned} \text{min:}\quad & \mathrm{Tr}(H) \\ \text{s.t.:}\quad & H - p_k \rho_k \in \mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}) \\ & \qquad (k = 1, \ldots, N), \\ & H \in \mathrm{Herm}(\mathcal{X}). \end{aligned}$$

~~Cone~~ Semidefinite program for PPT distinguishability

Primal (PPT)

$$\begin{aligned}\text{max:}\quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\ \text{s.t.:}\quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}}, \\ & \mu : \{1, \dots, N\} \rightarrow \mathrm{PPT}(\mathcal{X} : \mathcal{Y})\end{aligned}$$

Dual (PPT)

$$\begin{aligned}\text{min:}\quad & \mathrm{Tr}(H) \\ \text{s.t.:}\quad & H - p_k \rho_k \in \boxed{\mathrm{PPT}^*(\mathcal{X} : \mathcal{Y})} \\ & \qquad (k = 1, \dots, N), \\ & H \in \mathrm{Herm}(\mathcal{X}).\end{aligned}$$

Decomposable operators

- By definition,

$$\mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}) = \{S + \mathsf{T}_{\mathcal{X}}(R) \;:\; S, R \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})\}$$

- Choi-isomorphic to *decomposable maps*

$$\Phi(Y) = \Psi(Y) + (\mathsf{T} \circ \Xi)(Y), \qquad \Psi, \Xi \text{ completely positive}$$

Cone program for separable distinguishability

<u>Primal (Separable)</u>

$$\begin{aligned}
\text{max:}\quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\
\text{s.t.:}\quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}}, \\
& \mu : \{1, \ldots, N\} \rightarrow \mathrm{Sep}(\mathcal{X} : \mathcal{Y}).
\end{aligned}$$

<u>Dual (Separable)</u>

$$\begin{aligned}
\text{min:}\quad & \mathrm{Tr}(H) \\
\text{s.t.:}\quad & H - p_k\rho_k \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}) \\
& \qquad (k = 1, \ldots, N), \\
& H \in \mathrm{Herm}(\mathcal{X}).
\end{aligned}$$

Cone program for separable distinguishability

Primal (Separable)

$$\begin{aligned}\text{max:}\quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k)\rangle,\\ \text{s.t.:}\quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}},\\ & \mu : \{1,\ldots,N\} \to \mathrm{Sep}(\mathcal{X}:\mathcal{Y}).\end{aligned}$$

Dual (Separable)

$$\begin{aligned}\text{min:}\quad & \mathrm{Tr}(H)\\ \text{s.t.:}\quad & H - p_k\rho_k \in \boxed{\mathrm{Sep}^*(\mathcal{X}:\mathcal{Y})}\\ & \qquad (k = 1,\ldots,N),\\ & H \in \mathrm{Herm}(\mathcal{X}).\end{aligned}$$

Block-positive operators

- Choi representation of positive linear mappings:

$$\Phi(Y) \in \mathrm{Pos}(\mathcal{X}), \quad \text{for every } Y \in \mathrm{Pos}(\mathcal{Y})$$

- $\mathrm{Sep}^*(\mathcal{X}:\mathcal{Y}) \setminus \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y})$ are the *entanglement witnesses*

Benefits of the cone programming formulation

Analytically

- To prove a set is *not perfectly* distinguishable, we find H s.t.
  1. $\mathrm{Tr}(H) < 1$
  2. $H - p_k \rho_k \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$, for <u>all</u> $k \in \{1, \ldots, N\}$
- Many families of operators in $\mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$ are known
- Actual numerical bounds, as opposed to qualitative statements

Numerically

- We can approximate the Sep cone program by a hierarchy of semidefinite programs
- A MATLAB implementation is now in N. Johnston's QETLAB

Applications

Entanglement cost of distinguishing Bell states

- Max. prob. to LOCC-distinguish the 4 Bell states is $1/2$
- Max. prob. to LOCC-distinguish any set of 3 Bell states is $2/3$

Entanglement cost

Alice and Bob are given as a resource a 2-qubit entangled state

$$|\tau_\varepsilon\rangle = \sqrt{\frac{1+\varepsilon}{2}}\,|0\rangle|0\rangle + \sqrt{\frac{1-\varepsilon}{2}}\,|1\rangle|1\rangle, \qquad \varepsilon \in [0,1]$$

- Up to local unitaries, it characterizes all 2-qubit states
- 4 Bell states: *perfect* LOCC-disting. iff $\varepsilon = 0$ [HSSH, '03]
- 3 Bell states: *perfect* PPT-disting. iff $\varepsilon \leq 1/3$ [YDY, '14]
- 3 Bell states: what about separable and LOCC?

Entanglement cost of distinguishing Bell states

Theorem (new)

The maximum probability of distinguishing 3 Bell states is

$$\frac{1}{3}\left(2+\sqrt{1-\varepsilon^2}\right).$$

Corollary

1. *Max. ent. state ($\varepsilon = 0$) is necessary for perfect discrimination*
2. *Teleportation is optimal*

Corresponding map

A new positive map from $\mathrm{L}(\mathbb{C}^2 \oplus \mathbb{C}^2)$ to $\mathrm{L}(\mathbb{C}^2 \oplus \mathbb{C}^2)$

Local distinguishability of maximally entangled states

- N max. ent. states in $\mathbb{C}^d \otimes \mathbb{C}^d$ (what's the role of d?)
- A significant case because of the dual role of entanglement

	PPT	LOCC	References
$N = 2$, any d	—	*all* dist.	[Walgate et al., 2000]
$N = 3 = d$	—	*all* dist.	[Nathanson, 2005]
$N = 4 = d$	*some* indist.	—	[Yu, Duan, and Ying, 2012]
$4 < N < d$	*some* indist.	—	*this thesis*
$N > d$	*all* indist.	—	[Yu, Duan, and Ying, 2012, Duan et al. 2009, Ghosh et al. 2004]

Yu–Duan–Ying states

Theorem (YDY, '12)

The following 4 orthogonal max. ent. states in $\mathbb{C}^4 \otimes \mathbb{C}^4$ *are not perfectly distinguishable by PPT (and therefore LOCC):*

$$\begin{aligned} \phi_1 &= \psi_0 \otimes \psi_0 \\ \phi_2 &= \psi_1 \otimes \psi_1 \\ \phi_3 &= \psi_2 \otimes \psi_1 \\ \phi_4 &= \psi_3 \otimes \psi_1 \end{aligned}$$

Theorem (new)

The optimal probability of distinguishing YDY by LOCC is $3/4$.

Corresponding map

Breuer-Hall positive linear maps from $\mathrm{L}(\mathbb{C}^4)$ to $\mathrm{L}(\mathbb{C}^4)$

Small sets of locally indistinguishable max. ent. states

	PPT	LOCC	References
$N = 2$, any d	—	*all* dist.	[Walgate et al., 2000]
$N = 3 = d$	—	*all* dist.	[Nathanson, 2005]
$N = 4 = d$	*some* indist.	—	[Yu, Duan, and Ying, 2012]
$4 < N < d$	*some* indist.	—	*this thesis*
$N > d$	*all* indist.	—	[GKRS '04, DFXY '09, YDY '12]

Theorem (new)

There exists an indistinguishable set of $N < d$ maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$

Small sets of locally indistinguishable max. ent. states

Generalized Yu–Duan–Ying

$$\begin{aligned} \phi_1 &= \psi_0 \otimes \psi_0 \otimes \psi_0 & \phi_5 &= \psi_1 \otimes \psi_0 \otimes \psi_0 \\ \phi_2 &= \psi_0 \otimes \psi_1 \otimes \psi_1 & \phi_6 &= \psi_1 \otimes \psi_1 \otimes \psi_1 \\ \phi_3 &= \psi_0 \otimes \psi_2 \otimes \psi_1 & \phi_7 &= \psi_1 \otimes \psi_2 \otimes \psi_1 \\ \phi_4 &= \psi_0 \otimes \psi_3 \otimes \psi_1 & & \cancel{\phi_8 = \psi_1 \otimes \psi_3 \otimes \psi_1} \end{aligned}$$

- 7 orthogonal maximally entangled states in $\mathbb{C}^8 \otimes \mathbb{C}^8$
- Maximum probability for any separable measurement is $6/7$
- Perfectly distinguishable by PPT

Distinguishability of unextendable product sets

Definition (Unextendable product sets – UPS)

An orthonormal collection of product vectors

$$\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y}$$

s.t. there is no (nonzero) product vector $u \otimes v \perp \mathcal{A}$.

Previously known

- no UPS can be perfectly distinguished by LOCC meas.
- every UPS can be perfectly distinguished by PPT meas.
- every UPS in $\mathbb{C}^3 \otimes \mathbb{C}^3$ can be perfectly distinguished by separable meas.

UPS indistinguishable by separable measurements

Theorem (new)

Feng's UPS in $\mathbb{C}^4 \otimes \mathbb{C}^4$ *is not perfectly distinguishable by Sep.*

$$
\begin{aligned}
|\phi_1\rangle &= |0\rangle|0\rangle, \\
|\phi_2\rangle &= |1\rangle\left(|0\rangle - |2\rangle + |3\rangle\right)/\sqrt{3}, \\
|\phi_3\rangle &= |2\rangle\left(|0\rangle + |1\rangle - |3\rangle\right)/\sqrt{3}, \\
|\phi_4\rangle &= |3\rangle|3\rangle, \\
|\phi_5\rangle &= \left(|1\rangle + |2\rangle + |3\rangle\right)\left(|0\rangle - |1\rangle + |2\rangle\right)/3, \\
|\phi_6\rangle &= \left(|0\rangle - |2\rangle + |3\rangle\right)|2\rangle/\sqrt{3}, \\
|\phi_7\rangle &= \left(|0\rangle + |1\rangle - |3\rangle\right)|1\rangle/\sqrt{3}, \\
|\phi_8\rangle &= \left(|0\rangle - |1\rangle + |2\rangle\right)\left(|0\rangle + |1\rangle + |2\rangle\right)/3.
\end{aligned}
$$

Proof

- Not the usual cone program this time...
- ...but a criterion for perfect separable discrimination of UPS checkable with a *linear program*!

Conclusions

Contributions of the thesis

- A framework based on cone programming to test local distinguishability of quantum states
- Precise (often optimal) numerical bounds on the success probability of distinguishing some famous sets of states
- A novel connection between quantum state distinguishability and the study of positive linear maps

"State discrimination is the most fundamental task in physics."

— Jon Walgate (Calgary, 2005)

Open questions

- The other way: new sets of indistinguishable states from known positive maps?
- What about a cone program for LOCC...

Dual

$$
\begin{aligned}
\text{min:} \quad & \mathrm{Tr}(H) \\
\text{s.t.:} \quad & \begin{pmatrix} H - p_1\rho_1 & & \\ & \ddots & \\ & & H - p_N\rho_N \end{pmatrix} \in \boxed{\mathrm{Meas}^*_{\mathrm{LOCC}}(N, \mathcal{X} : \mathcal{Y})},
\end{aligned}
$$

Can we say anything about $\mathrm{Meas}^*_{\mathrm{LOCC}}(N, \mathcal{X} : \mathcal{Y})$?

- Other settings (multipartite, two copies, etc.)

Acknowledgments

Supervisor	John Watrous
Committee members	Richard Cleve Runyao Duan Debbie Leung Ashwin Nayak
Co-authors	Som Bandyopadhyay Nathaniel Johnston Vincent Russo Nengkun Yu
Funded by	NSERC US Army Research Office David R. Cheriton Scholarship

Publications

- A. Cosentino.
  PPT-indistinguishable states via semidefinite programming.
  Physical Review A, 2013.

- A. Cosentino and V. Russo.
  Small sets of locally indistinguishable orthogonal maximally entangled states.
  Quantum Information & Computation, 2014.

- S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu.
  Limitations on separable measurements by convex optimization.
  IEEE Transactions on Information Theory, 2015.