Small Sets of Locally Indistinguishable Orthogonal Maximally Entangled States

Alessandro Cosentino, Vincent Russo (arXiv:1307.3232)

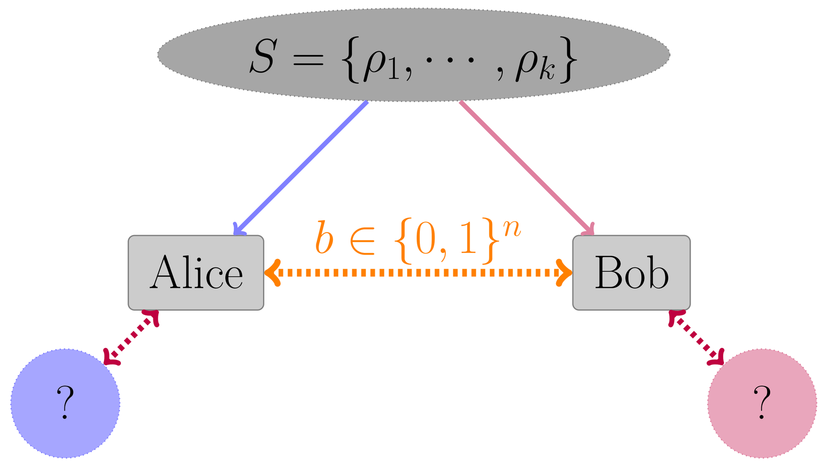
David R. Cheriton School of Computer Science and Institute for Quantum Computing
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

Introduction

- The state ρ_j from a set $S = \{\rho_1, \cdots, \rho_k\}$ is given to Alice and Bob, i.e., $\rho_j \in \mathrm{D}(\mathcal{A} \otimes \mathcal{B})$
- Alice and Bob can only use *Local quantum Operations and Classical Communication (LOCC)*

Setting:
Orthogonal states
Focus on *perfect* distinguishability
Drawn from a *uniform* probability distribution

Motivation: Understand non-locality and entanglement



Applications: Quantum cryptographic primitives, such as data hiding, secret sharing, etc.

Background

k – the size of the set ($|S| = k$)
d – local dimension (states lying in $\mathbb{C}^d \otimes \mathbb{C}^d$).

Distinguishable
- *any* 2 pure states [4]
- *any* 3 maximally entangled states, $d = 3$ [5]

Indistinguishable
- *any* k maximally entangled states when $k > d$ [1]
- 9 product states, $d = 3$ [6]

Question: What about $k < d$ maximally entangled states? ($d \geq 4$)

Notation

Transpose: $X \in \mathrm{L}(\mathcal{A})$, $\mathrm{T}(X) = X^{\mathrm{T}}$
Partial Transpose: $X \in \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$, $\mathrm{T}_{\mathcal{A}}(X) = (\mathrm{T} \otimes \mathbb{1}_{\mathcal{B}})(X)$

PPT operator: $P \geq 0$ such that $\mathrm{T}_{\mathcal{A}}(P) \geq 0$ (symmetric w.r.t. $\mathcal{A}$ and $\mathcal{B}$)
PPT measurement: Measurement whose operators are PPT

- The four Bell states form a locally indistinguishable set.

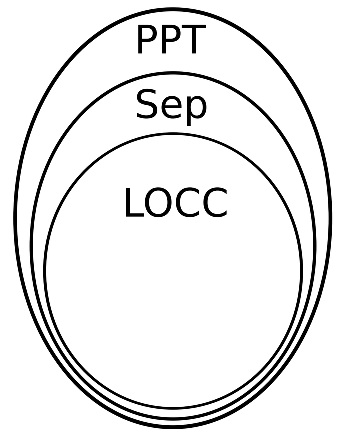
$$|\psi_0\rangle = |00\rangle + |11\rangle \qquad |\psi_1\rangle = |01\rangle + |10\rangle$$
$$|\psi_2\rangle = |01\rangle - |10\rangle \qquad |\psi_3\rangle = |00\rangle - |11\rangle$$

For $\mathcal{A} = \mathcal{B} = \mathbb{C}^2$, we denote $\psi_i = |\psi_i\rangle\langle\psi_i| \in \mathrm{D}(\mathcal{A} \otimes \mathcal{B})$.

Main Result

There exists a set of $k < d$ orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ that cannot be perfectly distinguished by LOCC.

Classes of Measurements



LOCC difficult objects to handle mathematically: difficult to design protocols, difficult to prove bounds on their power
Separable nicer structure than LOCC; optimizing over this set is NP-hard
PPT nice structure; efficient optimization via SDP

Semidefinite Programming (SDP)

- A generalization of linear programming
- A powerful tool with many applications in quantum information
- SDPs are efficiently solvable (polynomial time)
- Software packages available to solve SDPs
- Duality theory:

Primal problem	Dual problem
maximize: $\langle A, X\rangle$	minimize: $\langle B, Y\rangle$
subject to: $\Phi(X) = B$,	subject to: $\Phi^*(Y) \geq A$,
$X \in \mathrm{Pos}(\mathcal{X})$.	$Y \in \mathrm{Herm}(\mathcal{Y})$.
Optimum value: α	β

Weak Duality Theorem: For every SDP, $\alpha \leq \beta$.

Semidefinite Program for Distinguishing Quantum States via PPT

The maximum probability of distinguishing a set of states $\rho_j \in \{\rho_1, \cdots, \rho_k\}$ by PPT measurements can be expressed as the optimal value of an SDP:

Primal problem

$$\begin{aligned} \text{maximize:} \quad & \frac{1}{k}\sum_{j=1}^{k} \langle P_j, \rho_j\rangle \\ \text{subject to:} \quad & P_1 + \cdots + P_k = \mathbb{1}_{\mathcal{A}} \otimes \mathbb{1}_{\mathcal{B}}, \\ & P_1, \ldots, P_k \geq 0, \\ & \mathrm{T}_{\mathcal{A}}(P_1), \ldots, \mathrm{T}_{\mathcal{A}}(P_k) \geq 0. \end{aligned}$$

Dual problem

$$\begin{aligned} \text{minimize:} \quad & \frac{1}{k}\mathrm{Tr}(Y) \\ \text{subject to:} \quad & Y - \rho_j \geq \mathrm{T}_{\mathcal{A}}(Q_j), \quad j = 1, \ldots, k, \\ & Y \in \mathrm{Herm}(\mathcal{A} \otimes \mathcal{B}), \\ & Q_1, \ldots, Q_k \geq 0. \end{aligned}$$

Construction of States

Construction of $d = 2^t$ states in $\mathbb{C}^d \otimes \mathbb{C}^d$, by recursion on t.

Base case ($t = 2$) Set of states from [2]:

$$\rho_1^{(2)} = \psi_0 \otimes \psi_0, \quad \rho_3^{(2)} = \psi_2 \otimes \psi_1,$$
$$\rho_2^{(2)} = \psi_1 \otimes \psi_1, \quad \rho_4^{(2)} = \psi_3 \otimes \psi_1.$$

Recursive step ($t \geq 3$)

$$\rho_j^{(t)} = \begin{cases} \psi_0 \otimes \rho_j^{(t-1)} & \text{if } j \leq 2^{t-1}, \\ \psi_1 \otimes \rho_{j-2^{t-1}}^{(t-1)} & \text{if } j > 2^{t-1}. \end{cases}$$

If we only have to distinguish k of the states, the size of these sets can be as small as $C \cdot d/k$, where $C < 1$ is a constant.

Proof

- We exhibit a recursive solution for the dual:

Base case ($t = 2$) Explicit value for $Y^{(2)}, Q_1^{(2)}, Q_2^{(2)}, Q_3^{(2)}, Q_4^{(2)}$ (see paper for details)

Recursive step ($t \geq 3$)

$$Y^{(t)} = (\psi_0 + \psi_1)^{\otimes(t-2)} \otimes Y^{(2)},$$
$$Q_j^{(t)} = (\psi_0 + \psi_1)^{\otimes(t-2)} \otimes Q_r^{(2)},$$

where $r \equiv j \pmod 4$.

- Proof by induction that this solution satisfies the constraint

$$Y^{(t)} - \rho_j^{(t)} \geq \mathrm{T}_{\mathcal{A}}(Q_j^{(t)}),$$

for $j = 1, \ldots, k$. It holds, because $\mathrm{T}_{\mathcal{A}}(\psi_0 + \psi_1) = \psi_0 + \psi_1$.

Example in $\mathbb{C}^{16} \otimes \mathbb{C}^{16}$

- Probability of distinguishing this set of $k = 15$ states by PPT measurement is less than or equal to 14/15.

$$\begin{aligned}
\rho_1^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_0 \otimes \psi_0, & \rho_2^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_1 \otimes \psi_1 \\
\rho_3^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_2 \otimes \psi_1, & \rho_4^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_3 \otimes \psi_1 \\
\rho_5^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_0 \otimes \psi_0, & \rho_6^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_1 \otimes \psi_1 \\
\rho_7^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_2 \otimes \psi_1, & \rho_8^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_3 \otimes \psi_1 \\
\rho_9^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_0 \otimes \psi_0, & \rho_{10}^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_1 \otimes \psi_1 \\
\rho_{11}^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_2 \otimes \psi_1, & \rho_{12}^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_3 \otimes \psi_1 \\
\rho_{13}^{(4)} &= \psi_1 \otimes \psi_1 \otimes \psi_0 \otimes \psi_0, & \rho_{14}^{(4)} &= \psi_1 \otimes \psi_1 \otimes \psi_1 \otimes \psi_1 \\
& & \rho_{15}^{(4)} &= \psi_1 \otimes \psi_1 \otimes \psi_2 \otimes \psi_1
\end{aligned}$$

Open Problems

- Construction of indistinguishable sets with size $o(d)$?
- Construction that also works when d is not a power of two?
- Stronger bounds for the class of LOCC or separable measurements?

Software

Python script that generates the states and runs the optimization solver:
- https://bitbucket.org/acosenti/ppt-sdp-paper

References

[1] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, (2004).
[2] N. Yu, R. Duan and M. Ying, Phys. Rev. Letters **109**, (2012).
[3] A. Cosentino, Phys. Rev. A **87**, (2013).
[4] J. Walgate and L. Hardy, Phys. Rev. Letters **89**, (2002).
[5] M. Nathanson, J. Math. Phys., **46**, (2005).
[6] C. Bennett, D. DiVincenzo, C. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. Wootters, Phys. Rev. A **59**, (1999).

Acknowledgments

This research was supported by Canada's NSERC, the US ARO, and the David R. Cheriton Graduate Scholarship.

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing