Operator Algebras, Graph Theory, and Distinguishing Quantum States with LOCC

David Kribs

IWOTA Lancaster 2021
Operator Algebras to Geometric Rigidity
Session to Honour Prof. Stephen Power's Retirement

UNIVERSITY of GUELPH
CHANGING LIVES IMPROVING LIFE

Outline

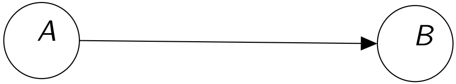
Outline

Quantum Local Operations and Classical Communication (LOCC)

- **Local Operations and Classical Communication (LOCC)** basic idea: multiple parties share set of quantum states spread across their subsystems, on which each party can perform local *quantum* operations, and then transmit their results only using *classical* information.
- The LOCC paradigm is fundamental in QIT; e.g., hybrid classical-quantum communication networks, probing locality vs quantum entanglement, power of distributed quantum algorithms, quantum teleportation protocols, etc.
- The key general LOCC problem we focus on here: **distinguishing quantum states** amongst a set of known states, where two parties (A, B) can perform quantum measurements on their individual subsystems, and then communicate classically.

Quantum LOCC

- Further, as arbitrary LOCC operations are notoriously difficult to characterize mathematically, we restrict ourselves to the case of **one-way LOCC**, where the communication is limited to one predetermined direction. This still captures many key examples and settings (though not all).
- One-way local operations and classical communication as a simple visual:



Bipartite Case

- Two parties A, B are separated at distance labs.
- They control their (finite dimensional) subsystem Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$.
- $\mathcal{H}_A \otimes \mathcal{H}_B$ is prepared in a pure state from a known set of states (unit vectors) $\mathcal{S} = \{|\psi_j\rangle\}_j$.
- Identify the particular j using one-way LOCC.

One-way LOCC Measurements

Mathematical description of one-way LOCC

A **one-way LOCC measurement** (with A going first) is a set of positive operators $\mathbb{M} = \{A_k \otimes B_{k,j}\}_{k,j}$ such that

$$\sum_k A_k = I_A \quad \text{and} \quad \sum_j B_{k,j} = I_B \quad \forall k.$$

$\Rightarrow$ If outcome $A_k \otimes B_{k,j}$ is obtained for some k and j, the conclusion is the prepared state was the one identified with the pair k, j.

One-way LOCC

Example (Easy one – Bell basis states)

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right) \end{aligned}$$

Here:

- Alice: $A_1 = |0\rangle\langle 0|$ and $A_2 = |1\rangle\langle 1|$.
- Bob: $\{B_{1,1}, B_{1,2}\} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} = \{B_{2,1}, B_{2,2}\}$.
- If Alice gets outcome 0, then tells Bob, who after measurement gets outcome 0, then the state is $|\psi_0\rangle$. Similarly it would be $|\psi_1\rangle$ if Bob measured a 1.

Operator relations for one-way LOCC

$\Rightarrow$ Let $|\Phi\rangle$ be the standard *maximally entangled state* on two-qudit space $\mathbb{C}^d \otimes \mathbb{C}^d$; $|\Phi\rangle = \frac{1}{\sqrt{d}}\big(|0\rangle|0\rangle + \ldots + |d-1\rangle|d-1\rangle\big)$. (A state $(I \otimes U)|\Phi\rangle$ is maximally entangled precisely when U is unitary.)

Theorem (Nathanson '13)

Let $\mathcal{S} = \{|\psi_i\rangle = (I \otimes U_i)|\Phi\rangle\} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$ be a set of orthogonal states (with U_i operators on $\mathbb{C}^d$). Then TFAE:

- *(i) The elements of $\mathcal{S}$ can be distinguished with one-way LOCC.*
- *(ii) There exists a set of states $\{|\phi_k\rangle\}_{k=1}^{r} \subseteq \mathbb{C}^d$ and positive numbers $\{m_k\}$ such that $\sum_k m_k|\phi_k\rangle\langle\phi_k| = I$ and for all k and $i \neq j$,*

$$\langle \phi_\mathbf{k} | \mathbf{U_j^* U_i} | \phi_\mathbf{k} \rangle = \mathbf{0}.$$

Operator relations for one-way LOCC

In the example above...

Example

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = (I_2 \otimes I_2)|\Phi\rangle$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = (I_2 \otimes X)|\Phi\rangle,$$

where X is the single-qubit Pauli bit flip operator. Here we have $U_1 = I_2$, $U_2 = X$, and the diagonal entries are zero;

$$U_j^* U_i = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Outline

Some Important Operator Structures

⇒ Recall the basic structure theory for *finite-dimensional C^*-algebras*: every such algebra $\mathfrak{A}$ is unitarily equivalent to an orthogonal direct sum of the form $\bigoplus_k (M_{m_k}(\mathbb{C}) \otimes I_{n_k})$.

Definition

Let $\mathfrak{A}$ be a unital C^*-algebra. Any linear subspace $\mathfrak{S}$ contained in $\mathfrak{A}$ which contains the identity and is closed under taking adjoints is called an **operator system**.

Definition

Let $\mathcal{H}$ be a Hilbert space and let $\mathfrak{S} \subseteq B(\mathcal{H})$ be a set of operators on $\mathcal{H}$ that form an operator system. A vector $|\psi\rangle \in \mathcal{H}$ is said to be a **separating vector** *of $\mathfrak{S}$ if $A|\psi\rangle \neq 0$ whenever A is a nonzero element of $\mathfrak{S}$.*

Some Important Operator Structures

$\Rightarrow$ If $\mathcal{H}$ is finite-dimensional and $\mathfrak{S}$ is in fact a C^*-subalgebra, then we may use the decomposition above for such algebras to determine the existence of a separating vector as follows.

Theorem (Pereira '03)

The C^*-algebra $\bigoplus_k (M_{m_k}(\mathbb{C}) \otimes I_{n_k})$ has a separating vector if and only if $n_k \geqslant m_k$ for all k.

E.g., In the case of the diagonal algebra $\mathfrak{A}_\Delta \cong \mathbb{C}^d$, $m_k = n_k = 1$ for all $1 \leqslant k \leqslant d$, and hence $\mathfrak{A}_\Delta$ has a separating vector, for example: $|\psi\rangle = \frac{1}{\sqrt{d}}(|0\rangle + \ldots + |d-1\rangle)$ does the job.

Taken together, these notions and our early results led to...

Operator Structure – LOCC Result

Theorem

Suppose the operator system $\mathfrak{S}_0 = \operatorname{span}\{U_i^* U_j, I\}_{i\neq j}$ *is closed under multiplication and hence is a* C^**-algebra. Then* $\mathcal{S} = \{(I\otimes U_i)|\Phi\rangle\}$ *is distinguishable by one-way LOCC if and only if* $\mathfrak{S}_0$ *has a separating vector.*

E.g., Road Map for Examples from Operator Structures:

- If we have $\mathfrak{A} = \operatorname{Alg}(\mathfrak{S}_0) \cong \oplus_k (M_{m_k} \otimes I_{n_k})$, then $\mathfrak{A}$ has a separating vector if and only if $n_k \geqslant m_k$ for all k.

- $\Rightarrow$ To find sets of *indistinguishable states*, we can look for sets $\{U_i\}$ such that $\mathfrak{S}_0 = \mathfrak{A}$ and $m_k > n_k$ for some k.

- $\Rightarrow$ We are led to consider sets of unitaries $\{U_i\}$, such that the set is (up to scalar multiples) closed under multiplication, taking *'s, and taking inverses.

Application: States from the Stabilizer Formalism

...Sets of such unitaries are plentiful in **Quantum Error Correction**...

Theorem

Let $\{U_i\}$ be a complete set of 4^k 'logical Pauli operators for a stabilizer k-qubit code' on $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$. Then $\mathcal{S} = \{(I \otimes U_i)|\Phi\rangle\}_i$ is distinguishable by one-way LOCC if and only if $k \leqslant \frac{n}{2}$.

Remark

The upper bound $(2k = n)$ gives sets that saturate a known bound for one-way distinguishable states on $\mathbb{C}^d \otimes \mathbb{C}^d$ $(d = 2^n)$. For $2k < n$, this produces (non-trivial) distinguishable sets; significant as it is known that many sets defined from $\mathcal{P}_n$ with $< 2^n$ operators (here $4^k < 2^n$) are *not* one-way distinguishable.

Outline

Graph Theory Nomenclature

- We write $G = (V, E)$ for a **simple graph** with vertex set V and edge set E. For $v, w \in V$, we write $v \sim w$ if the edge $\{v, w\} \in E$.
- The **complement** of G is the graph $\overline{G} = (V, \overline{E})$, where the edge set $\overline{E}$ consists of all two-element sets from V that are not in E.
- Another graph G' is a **subgraph** of G, written $G' \leqslant G$, if $V' \subseteq V$ and $E' \subseteq E$ with $v, w \in V'$ whenever $\{v, w\} \in E'$.
- A set of graphs $\{G_i = (V_i, E_i)\}$ **covers** G if $V = \cup_i V_i$ and $E = \cup_i E_i$, and $\{G_i\}$ is a **clique cover** for G if $\{G_i\}$ covers G and if each of the G_i is a complete graph (i.e., a clique).
- The **clique cover number** $\mathrm{cc}(G)$ is the smallest possible number of subgraphs contained in a clique cover of G.

Product States and Orthogonal Graph Representations

- Given a graph $G = (V, E)$, a function $\phi : V \to \mathbb{C}^d \backslash \{0\}$ is an **orthogonal representation** of G if for all vertices $v_i \neq v_j \in V$,

$$v_i \not\sim v_j \iff \langle \phi(v_i), \phi(v_j) \rangle = 0.$$

- Given a set of product states $\{|\psi_k^A\rangle \otimes |\psi_k^B\rangle\}_{k=1}^r$ on $\mathcal{H}_A \otimes \mathcal{H}_B$, Alice's graph is the unique graph $\mathbf{G_A}$ with $V = \{1, 2, \dots, r\}$ such that $k \mapsto |\psi_k^A\rangle$ is an orthogonal representation of G_A. Similarly, Bob's graph $\mathbf{G_B}$ is defined by orthogonality (or not) of the $|\psi_k^B\rangle$.

- By construction, the states are mutually orthogonal iff Alice's graph is a subgraph of the complement of Bob's graph; $G_A \leqslant \overline{G_B}$.

- E.g., $\mathcal{S} = \{|\psi_1\rangle = |00\rangle, |\psi_2\rangle = |01\rangle, |\psi_3\rangle = |10\rangle, |\psi_4\rangle = |11\rangle\}$. Then $V = \{1, 2, 3, 4\}$, $G_A = \{(1, 2), (3, 4)\}$, $G_B = \{(1, 3), (2, 4)\}$, and $\overline{G_B} = \{(1, 2), (3, 4), (2, 3), (1, 4)\}$.

One-Way LOCC Distinguishability of Product States via Graph Theory

Theorem

Given a set of product states in $\mathcal{H}_A \otimes \mathcal{H}_B$, let G_A and G_B be the graphs of the states from Alice and Bob's perspectives, respectively. Let $\phi : V_A \to \mathcal{H}_A$ be the association of vertices with Alice's states and assume that the set $\{\phi(v) : v \in V\}$ spans $\mathcal{H}_A$. Then the states are distinguishable with one-way LOCC with Alice measuring first if and only if there exists

(1) *a graph G satisfying $G_A \leqslant G \leqslant \overline{G_B}$,*

(2) *a clique cover $\{V_j\}_{j=1}^{k}$ of G, and,*

(3) *a POVM $\{Q_j\}$ on $\mathcal{H}_A$ such that for all $v \in V_A$, $Q_j\phi(v) \neq 0$ implies that $v \in V_j$.*

The Single Qubit Sender Case: Full Graph Characterisation

Theorem

A set of orthonormal product states in $\mathbb{C}^2 \otimes \mathbb{C}^d$, for $d \geqslant 2$, is distinguishable via one-way LOCC with Alice going first if and only if there is some graph between the two graphs G_A and $\overline{G_B}$ with clique cover number at most two; that is, there is a graph G such that

$$G_A \leqslant G \leqslant \overline{G_B} \quad \textit{and} \quad \mathrm{cc}\,(G) \leqslant 2. \tag{1}$$

- E.g., $\mathcal{S} = \{|\psi_1\rangle = |00\rangle, |\psi_2\rangle = |01\rangle, |\psi_3\rangle = |10\rangle, |\psi_4\rangle = |11\rangle\}$.

- $\Rightarrow$ This set is distinguishable with Alice going first, and can easily be seen to satisfy the theorem condition with:

$$G_A = G = \{(1,2),(3,4)\} \lneq \overline{G_B} = \{(1,2),(3,4),(2,3),(1,4)\},$$

and

$$\mathrm{cc}\,(G) = 2.$$

Outline

Conclusion & Outlook

- The use of techniques from **operator theory** and **operator algebras** in the subject of **LOCC** is relatively new, and our results on state distinguishability so far suggest some avenues worth pursuing further (e.g. connections with **quantum error correction**). We have obtained new results and examples, and new versions/realizations of previous results and examples.
- More recently, we have introduced **graph theory** techniques into our state distinguishability analysis, and we are continuing this work ...see references on the next slide.
- (Shameless extra plug) Generalization of Nielsen's Theorem on **LOCC state convertibility** ($\Leftrightarrow$ spectral **majorization**) to the **von Neumann algebra** framework: J.Crann, D.K., R.Levene, I.Todorov, Comm. Math. Phys., 378 (2020), 1123-1156.

References for our state distinguishability work

(also see references therein for other entrance points into literature)

- D.K., Comfort Mintah, Michael Nathanson, Rajesh Pereira, *Vector representations of graphs and distinguishing quantum product states with one-way LOCC*, Linear Algebra and its Applications, 602 (2020), 223-239.
- D.K., C.M., M.N., R.P., *One-way LOCC indistinguishable lattice states via operator structures*, Quantum Information Processing, 19 (2020), 194.
- D.K., C.M., M.N., R.P., *Quantum error correction and one-way LOCC*, Journal of Mathematical Physics, 60 (2019), 032202.
- D.K., C.M., M.N., R.P., *Operator structures and quantum LOCC conditions*, Journal of Mathematical Physics, 58 (2017), 092201.

(...and more to come)

Have A Nice Day

Thank you!