Mermin Non-Localty in Abstract Process Theories

Stefano Gogioso and William Zeng

Quantum Group
University of Oxford

15 July 2015
Introduction

- Mermin non-locality generalised to abstract process theories by [Coecke, Edwards, & Spekkens QPL ’09] and [Coecke, Duncan, Kissinger & Wang (2012)]
- a.k.a. Generalized Compositional Theories [1506.03632]
Introduction

- Mermin non-locality generalised to abstract process theories by [Coecke, Edwards, & Spekkens QPL ’09] and [Coecke, Duncan, Kissinger & Wang (2012)]
- a.k.a. Generalized Compositional Theories [1506.03632]
- Here we give the full necessary and sufficient conditions for Mermin non-locality of an abstract process theory:

  Mermin non-locality ⇐⇒ algebraically non-trivial phases
Introduction

- Mermin non-locality generalised to abstract process theories by [Coecke, Edwards, & Spekkens QPL ’09] and [Coecke, Duncan, Kissinger & Wang (2012)]
  - a.k.a. Generalized Compositional Theories [1506.03632]

- Here we give the full necessary and sufficient conditions for Mermin non-locality of an abstract process theory:

  \[
  \text{Mermin non-locality} \iff \text{algebraically non-trivial phases}
  \]

- Our work provides new experimental scenarios for the testing of non-locality, and novel insight into the security of certain Quantum Secret Sharing protocols.
Section 1

Mermin Measurements
A \textbf{†-Frobenius algebra} is a Frobenius algebra where the monoid \((\bigtriangleup, *)\) and the co-monoid \((\bigtriangledown, \ddagger)\) are adjoint.
A ↑-Frobenius algebra is a Frobenius algebra where the monoid \((\bigodot, \bullet)\) and the co-monoid \((\bigodot, \circlearrowright)\) are adjoint.

A ↑-Frobenius algebra is quasi-special if it is special up to some invertible scalar \(N\):

\[
\begin{array}{ccc}
\quad & \bigodot & \quad = \quad \bigodot \\
\quad & \circlearrowright & \quad = \quad \bigotimes N
\end{array}
\]
\(\dagger\)-Frobenius algebras

- A **\(\dagger\)-Frobenius algebra** is a Frobenius algebra where the monoid \((\bigotimes, \otimes)\) and the co-monoid \((\bigotimes', \otimes')\) are adjoint.

- A \(\dagger\)-Frobenius algebra is **quasi-special** if it is special up to some invertible scalar \(N\):

\[
\begin{align*}
\begin{array}{c}
\bullet \\
\end{array} &=
\begin{array}{c}
\bigotimes \\
\otimes \\
\end{array} =
\begin{array}{c}
N \\
\end{array}
\end{align*}
\]

- \(\dagger\)-qSCFA \(\equiv\) “quasi-special commutative \(\dagger\)-Frobenius algebra”

- Think of these as generalized orthogonal bases [0810.0812].
We will say that a pair of †-qSCFAs are **strongly complementary** if they satisfy the Hopf law and the following (unscaled) bialgebra equations:
The set of classical points (aka copyable states) $K_\circ$ of a $\dagger$-qSCFA are points $|\psi\rangle$ such that:
Classical Points

The set of classical points (aka copyable states) $K_\bullet$ of a $\dagger$-qSCFA $\bullet$ are points $|\psi\rangle$ such that:

\[
\psi = \psi^* = \psi
\]

A motivating intuition is to think of these as “basis element”-like.
Lemma

Let $(\bigcirc, \bullet)$ be a pair of strongly complementary $\dagger$-qSCFAs. Then the monoid $(\bigcirc, \bullet)$ acts as a group $K_{\bullet}$ on the classical points (aka copyable states) of $\bullet$, with the antipode $\circledast$ acting as inverse.
Lemma

Let $\bullet, \circ \circ$ be a pair of strongly complementary $\dagger$-qSCFAs. Then the monoid $(\bullet, \circ)$ acts as a group $K_\circ$ on the classical points (aka copyable states) of $\circ$, with the antipode $\tilde{\circ}$ acting as inverse.
A \( \bullet \)-phase, for a \( \uparrow \)-qSCFA \( \bullet \) on some object \( \mathcal{H} \), is a morphism \( \alpha : \mathcal{H} \to \mathcal{H} \) taking the following form for some state \( |\alpha\rangle \) of \( \mathcal{H} \):

\[
\alpha \ := \begin{array}{c}
\alpha \\
\downarrow \\
\alpha
\end{array}
\quad \text{where} \quad
\begin{array}{c}
\alpha \\
\downarrow \\
\alpha
\end{array} =
\begin{array}{c}
\alpha \\
\downarrow \\
\alpha
\end{array}
\]
A \textbullet{-phase}, for a \dagger{-qSCFA} \textbullet on some object \mathcal{H}, is a morphism \( \alpha : \mathcal{H} \rightarrow \mathcal{H} \) taking the following form for some state \( |\alpha\rangle \) of \( \mathcal{H} \): 

\[
\alpha := \begin{array}{c}
\alpha \\
\alpha
\end{array}
\]

where

\[
\begin{array}{c}
\alpha \\
\alpha
\end{array}
= \begin{array}{c}
\alpha \\
\alpha
\end{array}
\]

\[\text{Lemma}\]

Let \((\bullet, \bullet)\) be a pair of strongly complementary \dagger{-qSCFAs}. Then the monoid \((\bullet, \bullet)\) acts as a group \( P_\bullet \) on the \textbullet{-phases}, with the \textbullet{-classical points} \( K_\bullet \) as a subgroup.
GHZ States and Measurements

Definition

Given a †-qSFA ⊙ in a †-SMC, an \( N \)-partite GHZ state for ⊙ is:

\[
\text{n-systems}
\]
GHZ States and Measurements

Definition

Given a $\dagger$-qSFA $\bullet$ in a $\dagger$-SMC, an $N$-partite GHZ state for $\bullet$ is:

\[ \text{n-systems} \]

A measurement in $\dagger$-qSFA $\bullet$ “basis” is a doubled map (think of this as $X$).

\[ X := \text{boxed diagram} \]
GHZ States and Measurements

Definition

Given a ↑-qSFA \( \bullet \) in a ↑-SMC, an \( N \)-partite GHZ state for \( \bullet \) is:

\[
\text{n-systems}
\]

A measurement in ↑-qSFA \( \bullet \) “basis” is a doubled map (think of this as \( X \)). And prepending phases gives a new measurement (think \( Y \)). [1203.4988]

\[
X := \quad Y_\alpha :=
\]

\[
\alpha \
\]

\ [-\alpha ]
Let \((\circ, \bullet)\) be a pair of strongly complementary \(\dagger\)-qSCFAs. A **Mermin measurement** \((\alpha_1, ..., \alpha_N)\), for \(\bullet\)-phases \(\alpha_1, ..., \alpha_N\) with \(\sum_i \alpha_i\) is a \(\circ\)-classical point, is one taking the following form:
Let $(\circ, \bullet)$ be a pair of strongly complementary $\dagger$-qSCFAs. A **Mermin measurement** $(\alpha_1, ..., \alpha_N)$, for $\circ$-phases $\alpha_1, ..., \alpha_N$ with $\sum_i \alpha_i$ is a $\bullet$-classical point, is one taking the following form:

We will denote an ($N$-partite) **Mermin measurement scenario**, consisting of $S$ Mermin measurements, by $(\alpha_1^S, ..., \alpha_N^S)_{s=1,...,S}$. 
Section 2

Mermin Non-Localilty
Local Map

Let \((\alpha_1^s, ..., \alpha_N^s)_{s=1,...,S}\) be an \(N\)-partite Mermin measurement scenario, with \(\{a_1, ..., a_M\}\) the set of distinct \(\bullet\)-phases appearing.
Let \((\alpha_1^s, \ldots, \alpha_N^s)_{s=1,\ldots,S}\) be an \(N\)-partite Mermin measurement scenario, with \(\{a_1, \ldots, a_M\}\) the set of distinct •-phases appearing. The **local map** is the following morphism \(\mathcal{H} \otimes (M \cdot N) \to \mathcal{H} \otimes (N \cdot S)\):

\[
\begin{array}{ccc}
\alpha_1^1 & \cdots & \alpha_N^1 \\
\uparrow &   & \uparrow \\
\alpha_1^s & \cdots & \alpha_j^s \\
\uparrow &   & \uparrow \\
\alpha_1^S & \cdots & \alpha_N^S \\
\uparrow &   & \uparrow \\
a_1 & \cdots & a_M \\
\end{array}
\]

**Local Map**

Connected iff \(i = j\) and \(a_r = \alpha_j^s\)
A **local hidden variable model** for a Mermin measurement scenario \((\alpha_1^s, \ldots, \alpha_N^s)_{s=1,\ldots,S}\) is a state \(\Lambda’\) of \(\mathcal{H} \otimes (N \cdot S)\) such that:

\[
\forall s \in S, \begin{array}{c}
-\alpha_1^s \\
+\alpha_1^s \\
\vdots \\
-\alpha_N^s \\
+\alpha_N^s
\end{array}
\]

\(\Rightarrow\)

\(\forall s \in S, \begin{array}{c}
0 \\
0 \\
\vdots \\
0 \\
0
\end{array}\)

\(\Rightarrow\)

\(\forall s \in S, \Lambda’\)
Mermin non-locality

We say a $\dagger$-SMC $C$ is **Mermin local** if all Mermin measurement scenarios admit a local hidden variable model.
Mermin non-locality

- We say a $†$-SMC $C$ is **Mermin local** if all Mermin measurement scenarios admit a local hidden variable model.

- We say $C$ is **Mermin non-local** if there is some Mermin measurement scenario without a local hidden variable model.
Non-Trivial Algebraic Extensions

Definition

Let \((G, +, 0)\) be an abelian group and \((H, +, 0)\) be an abelian subgroup of \(G\). Then \(G\) is a **non-trivial algebraic extension** of \(H\) if there exists a finite system of equations \(\left( \sum_{r=1}^{M} n^s_r x_r = h^s \right)_s\), with \(h^s \in H\) and \(n^s_r \in \mathbb{Z}\), which has solutions in \(G\) but not in \(H\). Otherwise, we say \(G\) is a **trivial algebraic extension** of \(H\).
Consider the finite abelian group $G = (\{\pm 1, \pm i\}, \cdot, 1)$ and its subgroup $(\{\pm 1\}, \cdot, 1)$. Then the following equation has solution $x = i$ in $G$, but no solutions in $H$: $x^2 = -1$
Consider the finite abelian group $G = (\{\pm 1, \pm i\}, \cdot, 1)$ and its subgroup $(\{\pm 1\}, \cdot, 1)$. Then the following equation has solution $x = i$ in $G$, but no solutions in $H$:

$$x^2 = -1$$

On the other hand, if $G = K \times K'$ is an abelian group and $H = K \times \{0\}$, then every system of equations as per our definition will have solution in $G$ if and only if it does in $H$. 
Let \((\bullet, \circ)\) be a pair of strongly complementary \(\dagger\)-qSFAs. We say that the pair has **algebraically non-trivial phases** if the \(\bullet\)-phase group \(P_\bullet\) is a non-trivial algebraic extension of the subgroup \(K_\bullet\) of \(\circ\)-classical points.
Algebraically Non-Trivial Phases

- Let \((\bullet, \circlearrowleft)\) be a pair of strongly complementary \(\dagger\)-qSFAs. We say that the pair has **algebraically non-trivial phases** if the \(\bullet\)-phase group \(P\) is a non-trivial algebraic extension of the subgroup \(K\) of \(\circlearrowleft\)-classical points.

- For example, \((\bullet, \circlearrowleft)\) has an algebraically non-trivial phase \(\frac{\pi}{2}\) in the ZX calculus, where \(P \cong \mathbb{Z}_4\) and \(K \cong \mathbb{Z}_2\).
Algebraically Non-Trival Phases

Let $(\bigcirc, \bigcirc)$ be a pair of strongly complementary $\dagger$-qSFAs. We say that the pair has **algebraically non-trivial phases** if the $\bigcirc$-phase group $P_\bigcirc$ is a non-trivial algebraic extension of the subgroup $K_\bigcirc$ of $\bigcirc$-classical points.

For example, $(\bigcirc, \bigcirc)$ has an algebraically non-trivial phase $\pi/2$ in the ZX calculus, where $P_\bigcirc \cong \mathbb{Z}_4$ and $K_\bigcirc \cong \mathbb{Z}_2$.

On the other hand, it has no algebraically non-trivial phase in Spek, where $P_\bigcirc \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K_\bigcirc \cong \mathbb{Z}_2$. 
Section 3

Results
Theorem

Let $C$ be a $†$-SMC, and $(\bullet, \circ)$ be a strongly complementary pair of $†$-qSCFAs. Suppose further that the $\bullet$-classical points form a basis. If the group $P_\bullet$ is a non-trivial algebraic extension of the subgroup $K_\bullet$, then $C$ is Mermin non-local.
Mermin Non-Localility

**Theorem**

Let $\mathcal{C}$ be a $\dagger$-SMC, and $(\bullet, \circ)$ be a strongly complementary pair of $\dagger$-qSCFAs. Suppose further that the $\bullet$-classical points form a basis. If the group $P_{\bullet}$ is a non-trivial algebraic extension of the subgroup $K_{\bullet}$, then $\mathcal{C}$ is Mermin non-local.

**Corollary**

The ZX calculus is Mermin non-local, with $P_{\bullet} \cong \mathbb{Z}_4$ and $K_{\bullet} \cong \mathbb{Z}_2$. 
Theorem

Let $\mathcal{C}$ be a $\dagger$-SMC. Suppose that for every strongly complementary pair $\langle \bullet, \circ \rangle$ of $\dagger$-qSCFAs, the group $P_{\bullet}$ is a trivial algebraic extension of the subgroup $K_{\circ}$. Then $\mathcal{C}$ is Mermin local.
Theorem

Let $\mathcal{C}$ be a $\dagger$-SMC. Suppose that for every strongly complementary pair $(\bullet, \circ)$ of $\dagger$-qSCFAs, the group $P_{\bullet}$ is a trivial algebraic extension of the subgroup $K_{\circ}$. Then $\mathcal{C}$ is Mermin local.

Corollary

Spek is Mermin local, with $P_{\bullet} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K_{\circ} \cong \mathbb{Z}_2$. Confirms [Coecke et al. QPL ’09].
Theorem

Let \( \mathcal{C} \) be a \( \dagger \)-SMC. Suppose that for every strongly complementary pair \((\bullet, \bullet)\) of \( \dagger \)-qSCFAs, the group \( P_\bullet \) is a trivial algebraic extension of the subgroup \( K_\bullet \). Then \( \mathcal{C} \) is Mermin local.

Corollary

Spek is Mermin local, with \( P_\bullet \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \) and \( K_\bullet \cong \mathbb{Z}_2 \). Confirms [Coecke et al. QPL ’09].

Corollary

The category \( \text{fRel} \) is Mermin local, with \( P_\bullet \cong G^H \) and \( K_\bullet \cong G \) the subgroup of \( H \)-indexed vectors with all components equal.
1. The $N$-partite Mermin measurement given before is equivalent to the following state (by strong complementarity):

\[
-\alpha_1 \alpha_1 - \alpha_N \alpha_N = -\sum \alpha_i + \sum \alpha_i
\]
2. We can re-write the sum by grouping the $\circ$-phases and introducing integer coefficients:

$$\sum n_r a_r = \sum \alpha_i$$
2. We can re-write the sum by grouping the $\bullet$-phases and introducing integer coefficients:

$$
\sum_r n_r a_r = \sum_i \alpha_i
$$

3. If $a := \sum_i \alpha_i$, we can see the new sum as stating that the following equation is satisfied by setting $x_r = a_r$:

$$
\sum_r n_r x_r = a
$$
4. Consider the Mermin measurement scenario 
\((\alpha_1^s, \ldots, \alpha_N^s)_{s=1,\ldots,S}\), and the set \(\{a_1, \ldots, a_M\}\) of distinct \(s\)-phases appearing in it.
4. Consider the Mermin measurement scenario 
\((\alpha^s_1, \ldots, \alpha^s_N)_{s=1,\ldots,s}\), and the set \(\{a_1, \ldots, a_M\}\) of distinct \(\circ\)-phases appearing in it.

5. By defining \(a^s := \sum_i \alpha^s_i \in K\), we associate the following system of equations, satisfied by \(x_r = a_r\), to the scenario:

\[
\begin{align*}
\sum_{r=1}^{M} n_r^1 x_r &= a^1 \\
&\vdots \\
\sum_{r=1}^{M} n_r^S x_r &= a^S
\end{align*}
\]
6. Conversely, each system with \( a^1, ..., a^S \in K \) can be associated to a Mermin measurement scenario.
6. Conversely, each system with $a^1, \ldots, a^S \in K$ can be associated to a Mermin measurement scenario.

7. **Key result:** the existence of a local hidden variable model for a Mermin measurement scenario is equivalent to the existence of a $K$ solution for the associated system of equations.
6. Conversely, each system with $a^1, \ldots, a^S \in K$ can be associated to a Mermin measurement scenario.

7. **Key result:** the existence of a local hidden variable model for a Mermin measurement scenario is equivalent to the existence of a $K$ solution for the associated system of equations.

8. If all systems have such a $K$ solution, then all Mermin measurement scenarios have local hidden variable models.
6. Conversely, each system with \( a^1, \ldots, a^S \in K \) can be associated to a Mermin measurement scenario.

7. **Key result:** the existence of a local hidden variable model for a Mermin measurement scenario is equivalent to the existence of a \( K \) solution for the associated system of equations.

8. If all systems have such a \( K \) solution, then all Mermin measurement scenarios have local hidden variable models.

9. If some system does not admit a \( K \) solution, then (with enough \( \bullet \)-classical points) we construct a non-locality proof.
Applications

- The HBB CQ \((N, N)\) family of Quantum Secret Sharing protocols is directly based on Mermin non-locality. Our characterisation links the security of the protocols to algebraic non-triviality of the phases chosen.
Applications

- The HBB CQ \((N, N)\) family of Quantum Secret Sharing protocols is directly based on Mermin non-locality. Our characterisation links the security of the protocols to algebraic non-triviality of the phases chosen.

- Current literature includes the \((D + 1, 2, D)\) [Zukowski & Kaszlikowski (1999)], \((N > D, 2, D \text{ even})\) [Cerf & Pironio 2002], and \((\text{odd } N, 2, \text{even } D)\) [Lee et al. 2006].
Applications

- The HBB CQ \((N, N)\) family of Quantum Secret Sharing protocols is directly based on Mermin non-locality. Our characterisation links the security of the protocols to algebraic non-triviality of the phases chosen.

- Current literature includes the \((D + 1, 2, D)\) [Zukowski & Kaszlikowski (1999)], \((N > D, 2, D \text{ even})\) [Cerf & Pironio 2002], and \((\text{odd } N, 2, \text{ even } D)\) [Lee et al. 2006].

- These results Mermin measurement scenarios focus on the complementary XY pair of observables (i.e. the 0 and \(\pi/2\) Z-phases in the \(\mathbb{Z}_2\) case, or appropriate generalisations). Our work provides a wealth of additional scenarios for experimental testing of Mermin non-locality.
Conclusions

- We presented the full characterisation of Mermin non-locality:

Mermin non-locality $\iff$ algebraically non-trivial phases
We presented the full characterisation of Mermin non-locality:

Mermin non-locality $\iff$ algebraically non-trivial phases

We provided novel insight into the connection between non-locality and the security of certain quantum protocols.
We presented the full characterisation of Mermin non-locality:

\[
\text{Mermin non-locality } \iff \text{algebraically non-trivial phases}
\]

We provided novel insight into the connection between non-locality and the security of certain quantum protocols.

We dispelled the belief that complementarity of the observables pair plays a role in Mermin non-locality.
Thank You!

Thanks for Your Attention!

Any Questions?