Mermin Non-Locality in Abstract Process Theories

arXiv:1506.02675

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:

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

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

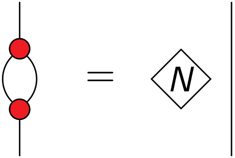
Mermin Measurements

†-Frobenius algebras

- A †-**Frobenius algebra** is a Frobenius algebra where the monoid ( , ) and the co-monoid ( , ) are adjoint.

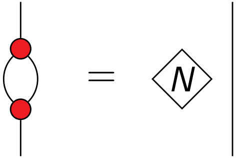
†-Frobenius algebras

- A †-**Frobenius algebra** is a Frobenius algebra where the monoid ( , ) and the co-monoid ( , ) are adjoint.
- A †-Frobenius algebra is **quasi-special** if it is special up to some invertible scalar N:



†-Frobenius algebras

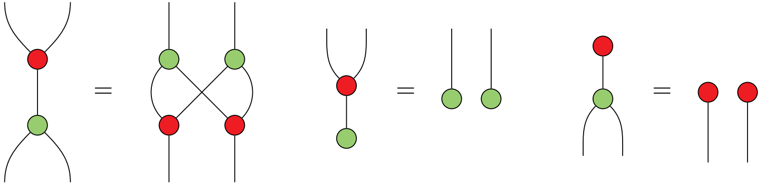
- A †-**Frobenius algebra** is a Frobenius algebra where the monoid ( , ) and the co-monoid ( , ) are adjoint.
- A †-Frobenius algebra is **quasi-special** if it is special up to some invertible scalar N:



- †-qSCFA ≡ "quasi-special commutative †-Frobenius algebra"
- Think of these as generalized orthogonal bases [0810.0812].

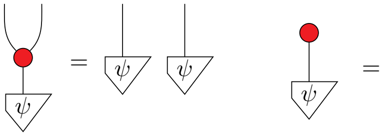
Strong Complementarity

We will say that a pair of †-qSCFAs are **strongly complementary** if they satisfy the Hopf law and the following (unscaled) bialgebra equations:



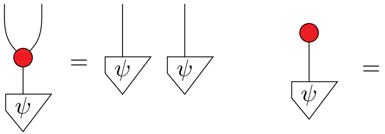
Classical Points

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



Classical Points

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



A motivating intuition is to think of these as "basis element"-like.

Group of Classical Points

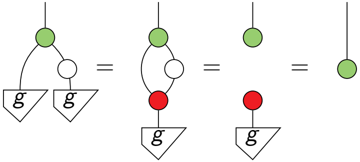
Lemma

Let (●, ●) be a pair of strongly complementary †-qSCFAs. Then the monoid (●, ●) acts as a group $K_●$ on the classical points (aka copyable states) of ●, with the antipode ○ acting as inverse.

Group of Classical Points

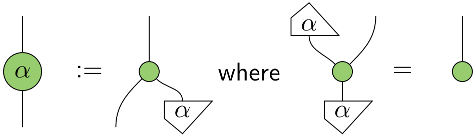
Lemma

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



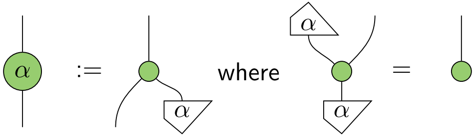
Phase Group

A ∘ **-phase**, for a †-qSCFA ∘ on some object $\mathcal{H}$, is a morphism $\alpha : \mathcal{H} \to \mathcal{H}$ taking the following form for some state $|\alpha\rangle$ of $\mathcal{H}$:



Phase Group

A ●-**phase**, for a †-qSCFA ● on some object $\mathcal{H}$, is a morphism $\alpha : \mathcal{H} \to \mathcal{H}$ taking the following form for some state $|\alpha\rangle$ of $\mathcal{H}$:



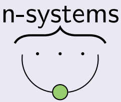
Lemma

Let (●, ●) be a pair of strongly complementary †-qSCFAs. Then the monoid (⅄, ⫯) acts as a group $P_{●}$ on the ●-phases, with the ●-classical points $K_{●}$ as a subgroup.

GHZ States and Measurements

Definition

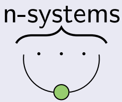
Given a †-qSFA ● in a †-SMC, an *N*-**partite GHZ state** for ● is:



GHZ States and Measurements

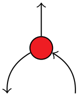
Definition

Given a †-qSFA ● in a †-SMC, an N-**partite GHZ state** for ● is:



A measurement in †-qSFA ● "basis" is a doubled map (think of this as X).

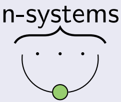
X :=



GHZ States and Measurements

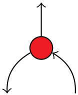
Definition

Given a †-qSFA ● in a †-SMC, an ***N*-partite GHZ state** for ● is:

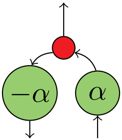


A measurement in †-qSFA ● "basis" is a doubled map (think of this as X). And prepending phases gives a new measurement (think Y). [1203.4988]

$X :=$

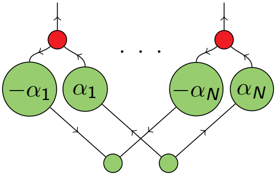


$Y_\alpha :=$



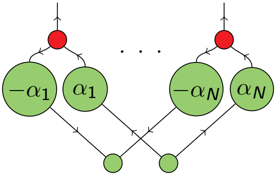
Mermin Measurements

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



Mermin Measurements

Let $({\color{green}\bullet}, {\color{red}\bullet})$ be a pair of strongly complementary †-qSCFAs.
A **Mermin measurement** $(\alpha_1, \ldots, \alpha_N)$, for ${\color{green}\bullet}$-phases $\alpha_1, \ldots, \alpha_N$ with $\sum_i \alpha_i$ is a ${\color{red}\bullet}$-classical point, is one taking the following form:



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

Section 2

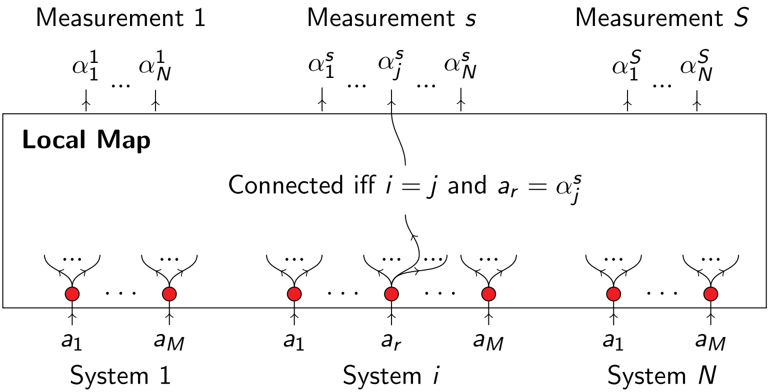
Mermin Non-Locality

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 ●-phases appearing.

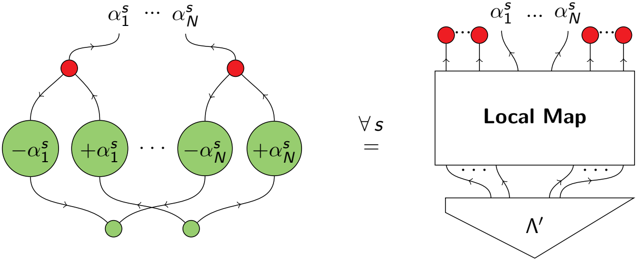
Local Map

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 ○-phases appearing. The **local map** is the following morphism $\mathcal{H}^{\otimes(M \cdot N)} \to \mathcal{H}^{\otimes(N \cdot S)}$:



Local Hidden Variables

A **local hidden variable model** for a Mermin measurement scenario $(\alpha_1^s, ..., \alpha_N^s)_{s=1,...,S}$ is a state Λ' of $\mathcal{H}^{\otimes(N \cdot S)}$ such that:



Mermin non-locality

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

Mermin non-locality

- We say a †-SMC $\mathcal{C}$ is **Mermin local** if all Mermin measurement scenarios admit a local hidden variable model.
- We say $\mathcal{C}$ 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 $(\sum_{r=1}^{M} n_r^s x_r = h^s)_s$, with $h^s \in H$ and $n_r^s \in \mathbb{Z}$, which has solutions in G but not in H. Otherwise, we say G is a **trivial algebraic extension** of H.

Non-Trivial Algebraic Extensions

- 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:

$$x^2 = -1$$

Non-Trivial Algebraic Extensions

- 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.

Algebraically Non-Trival Phases

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

Algebraically Non-Trival Phases

- Let $(\textcolor{green}{\bullet}, \textcolor{red}{\bullet})$ be a pair of strongly complementary †-qSFAs. We say that the pair has **algebraically non-trivial phases** if the $\textcolor{green}{\bullet}$-phase group $P_{\textcolor{green}{\bullet}}$ is a non-trivial algebraic extension of the subgroup $K_{\textcolor{red}{\bullet}}$ of $\textcolor{red}{\bullet}$-classical points.
- For example, $(\textcolor{green}{\bullet}, \textcolor{red}{\bullet})$ has an algebraically non-trivial phase $\pi/2$ in the ZX calculus, where $P_{\textcolor{green}{\bullet}} \cong \mathbb{Z}_4$ and $K_{\textcolor{red}{\bullet}} \cong \mathbb{Z}_2$.

Algebraically Non-Trival Phases

- Let $(\circ, \bullet)$ be a pair of strongly complementary †-qSFAs. We say that the pair has **algebraically non-trivial phases** if the $\circ$-phase group $P_{\circ}$ is a non-trivial algebraic extension of the subgroup $K_{\bullet}$ of $\bullet$-classical points.
- For example, $(\circ, \bullet)$ has an algebraically non-trivial phase $\pi/2$ in the ZX calculus, where $P_{\circ} \cong \mathbb{Z}_4$ and $K_{\bullet} \cong \mathbb{Z}_2$.
- On the other hand, it has no algebraically non-trivial phase in Spek, where $P_{\circ} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K_{\bullet} \cong \mathbb{Z}_2$.

Section 3

Results

Mermin Non-Locality

Theorem

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

Mermin Non-Locality

Theorem

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

Corollary

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

Mermin Locality

Theorem

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

Mermin Locality

Theorem

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

Corollary

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

Mermin Locality

Theorem

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

Corollary

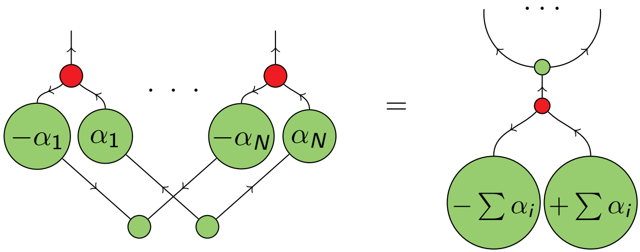
Spek is Mermin local, with $P_{\textcolor{green}{\bullet}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K_{\textcolor{red}{\bullet}} \cong \mathbb{Z}_2$. Confirms [Coecke et al. QPL '09].

Corollary

The category fRel *is Mermin local, with $P_{\textcolor{green}{\bullet}} \cong G^H$ and $K_{\textcolor{red}{\bullet}} \cong G$ the subgroup of H-indexed vectors with all components equal.*

Main Proof Concepts (1/4)

1. The N-partite Mermin measurement given before is equivalent to the following state (by strong complementarity):



Main Proof Concepts (2/4)

2. We can re-write the sum by grouping the ●-phases and introducing integer coefficients:

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

Main Proof Concepts (2/4)

2. We can re-write the sum by grouping the ●-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 $x_r = a_r$:

$$\sum_r n_r \, x_r = a$$

Main Proof Concepts (3/4)

4. Consider the Mermin measurement scenario $(\alpha_1^s, ..., \alpha_N^s)_{s=1,...,S}$, and the set $\{a_1, ..., a_M\}$ of distinct ○-phases appearing in it.

Main Proof Concepts (3/4)

4. Consider the Mermin measurement scenario $(\alpha_1^s, ..., \alpha_N^s)_{s=1,...,S}$, and the set $\{a_1, ..., a_M\}$ of distinct ●-phases appearing in it.
5. By defining $a^s := \sum_i \alpha_i^s \in K_{●}$, we associate the following system of equations, satisfied by $x_r = a_r$, to the scenario:

$$\begin{cases} \sum_{r=1}^{M} n_r^1 x_r &= a^1 \\ & \vdots \\ \sum_{r=1}^{M} n_r^S x_r &= a^S \end{cases}$$

Main Proof Concepts (4/4)

6. Conversely, each system with $a^1, ..., a^S \in K_{\bullet}$ can be associated to a Mermin measurement scenario.

Main Proof Concepts (4/4)

6. Conversely, each system with $a^1, ..., a^S \in K_{\bullet}$ 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 $K_{\bullet}$ solution for the associated system of equations.

Main Proof Concepts (4/4)

6. Conversely, each system with $a^1, ..., a^S \in K_{\bullet}$ 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 $K_{\bullet}$ solution for the associated system of equations.
8. If all systems have such a $K_{\bullet}$ solution, then all Mermin measurement scenarios have local hidden variable models.

Main Proof Concepts (4/4)

6. Conversely, each system with $a^1, ..., a^S \in K_{\bullet}$ 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 $K_{\bullet}$ solution for the associated system of equations.
8. If all systems have such a $K_{\bullet}$ solution, then all Mermin measurement scenarios have local hidden variable models.
9. If some system does not admit a $K_{\bullet}$ 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)], $(N > D, 2, D$ even) [Cerf & Pironio 2002], and (odd $N, 2,$ 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)], $(N > D, 2, D$ even) [Cerf & Pironio 2002], and (odd $N, 2,$ 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:

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

Conclusions

- 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.

Conclusions

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

$$\text{Mermin non-locality} \quad \Longleftrightarrow \quad \text{algebraically non-trivial phases}$$

- 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?