Mermin Non-Locality in Abstract Process Theories

Stefano Gogioso
Quantum Group
University of Oxford
stefano.gogioso@cs.ox.ac.uk

William Zeng
Quantum Group
University of Oxford
william.zeng@cs.ox.ac.uk

The study of non-locality is fundamental to the understanding of quantum mechanics. The past 50 years have seen a number of non-locality proofs, but its fundamental building blocks, and the exact role it plays in quantum protocols, has remained elusive. In this paper, we focus on a particular flavour of non-locality, generalising Mermin's argument on the GHZ state. Using strongly complementary observables, we provide necessary and sufficient conditions for Mermin non-locality in abstract process theories. We show that the existence of more phases than classical points (aka eigenstates) is not sufficient, and that the key to Mermin non-locality lies in the presence of certain algebraically non-trivial phases. This allows us to show that fRel, a favourite toy model for categorical quantum mechanics, is Mermin local. We show Mermin non-locality to be the key resource ensuring the device-independent security of the HBB CQ (N,N) family of Quantum Secret Sharing protocols. Finally, we challenge the unspoken assumption that the measurements involved in Mermin-type scenarios should be complementary (like the pair X,Y), opening the doors to a much wider class of potential experimental setups than currently employed. In short, we give conditions for Mermin non-locality tests on any number of systems, where each party has an arbitrary number of measurement choices, where each measurement has an arbitrary number of outcomes and further, that works in any abstract process theory.

PACS Numbers: 03.65.Fd,03.65.Ta,03.65.Ud, 03.67.Dd

1 Introduction

Non-locality is a fundamental property of quantum mechanics. It impacts both foundations and application, ruling out the existence of *local hidden variable theories* consistent with quantum theory [7], and underpinning protocols like quantum key distribution [14] and quantum secret sharing [21]. The importance of this property pushed the development of methods to characterise it both in general (e.g. the sheaf-theoretic methods of [2]) and in specific extensions of quantum theory (e.g. the generalized probabilistic theories of [6]).

We focus on a particular possibilistic class of non-locality arguments generalized from Mermin's argument [22] and related to the recent work on All-versus-Nothing arguments by Abramsky et al. [1]. These experiments produce possibilistic evidence for quantum mechanical non-locality, i.e. certain measurement outcomes that can only be realized by non-local theories. Mermin scenarios are typically described by triples (N,M,D) for N parties with M measurement choices for each party, each having D classical outcomes. Current literature generalises from the original $(3,2,2)$ scenario [22] to derive non-locality proofs for the $(3,3,2)$ [25], $(D+1,2,D)$ [29], $(N>D,2,D \text{ even})$ [23], and $(\text{odd } N,2,\text{even } D)$ [18]. One contribution of our work is to extend the work of [11] to cover all (N,M,D) scenarios.

In [11], Coecke et al. used strong complementarity to formulate Mermin arguments within the framework of Categorical Quantum Mechanics [3]. Not only does this approach help generalize non-locality arguments within quantum theory, but it also paved the way towards an understanding of Mermin non-locality in *abstract process theories*, aka dagger symmetric monoidal categories. As a corollary, they

Chris Heunen, Peter Selinger, and Jamie Vicary (Eds.): 12th International Workshop on Quantum Physics and Logic (QPL 2015).
EPTCS 195, 2015, pp. 228–246, doi:10.4204/EPTCS.195.17

© S. Gogioso & W. Zeng
This work is licensed under the Creative Commons Attribution-Noncommercial-Share Alike License.

are able to identify the difference between qubit stabilizer quantum mechanics (which is non-local) and Spekken's toy theory (which is local) in the structure of the respective phase groups [11, 12].

In Sections 3 and 4, we remove implicit assumptions about phase groups and classical points from [11] and use strongly complementary structures to generalise Mermin measurements to abstract process theories, defining Mermin non-locality as the existence of a Mermin measurement scenario not admitting a local hidden variable model.

In Section 4, we show that strong complementarity is not sufficient to characterise Mermin non-locality. The phase group structure is shown to provide necessary algebraic conditions in abstract process theories, as summarised by our first main result:

Theorem. 4.8. Let $\mathscr{C}$ be a †-SMC. If for any strongly complementary pair $(\circ, \bullet)$ of †-qSCFAs the group of $\circ$-phases is a trivial algebraic extension of the subgroup of $\bullet$-classical points (i.e. if there exist no algebraically non-trivial $\circ$-phases), then $\mathscr{C}$ is Mermin local.

Thus $\circ$-phase groups that are trivial algebraic extensions of the respective subgroups of $\bullet$-classical points always lead to local hidden variable models, irregardless of whether there are enough $\bullet$-classical points to form a basis and/or strictly more $\circ$-phases than $\bullet$-classical points. Indeed, we show that the category fRel of finite sets and relations is Mermin local (despite it having arbitrarily many more $\circ$-phases than $\bullet$-classical points), and also confirm that Spekken's toy theory is Mermin local (despite them having enough $\bullet$-classical points to form a basis). Our method also gives an easy proof that qutrit stabilizer mechanic is Mermin local.

Additionally, in Section 4, we show that the existence of algebraically non-trivial $\circ$-phases is sufficient, under mild additional assumptions, to formulate a non-locality argument. This leads to our second main result:

Theorem. 4.7. Let $\mathscr{C}$ be a †-SMC, and $(\circ, \bullet)$ be a strongly complementary pair of †-qSCFAs. Suppose further that the $\bullet$-classical points form a basis. If the group of $\circ$-phases is a non-trivial algebraic extension of the subgroup of $\bullet$-classical points, then $\mathscr{C}$ is Mermin non-local.

As a consequence, we confirm that qubit stabilizer quantum mechanics is Mermin non-local.

In Section 6, we argue that our concrete characterisation as the existence of algebraically non-trivial phases can be used to see Mermin non-locality as a resource in the construction of quantum protocols. We exemplify this by showing how the security of the HBB CQ (N,N) family of Quantum Secret Sharing protocols from [20, 21] directly relates to the flavour of non-locality explored in this work.

In Section 5, we use our general framework to investigate Mermin non-locality in fdHilb, the usual arena of quantum mechanics. The traditional formulation of Mermin arguments relies on sets of complementary measurements, such as the X ($\bullet$ measurement with $\circ$-phase 0) and Y ($\bullet$ measurement with $\circ$-phase $\frac{\pi}{2}$) measurements of the qubit in the original $(3,2,2)$ Mermin argument. We show how, even in the case of $(N,2,D)$ scenarios, many more possible measurements exist than complementary ones. This result opens a wealth of novel experimental configurations for tests of Mermin non-locality and, through results of Section 6, new configurations for quantum secret sharing protocols as well.

2 Background

This section refers the reader to background literature on the mathematical concepts of abstract process theories that we use in this work.

Classical structures, aka special commutative †-Frobenius algebras (†-SCFAs), play a central role in Categorical Quantum Mechanics (CQM) [3] as the abstract incarnation of non-degenerate observables.

The operational aspect of †-SCFAs is extensively covered in [9], where they are interpreted as models for the classical data operations of copy, deletion, and comparison. Their key connection with non-degenerate observables in quantum mechanics is provided by [13], where it is proven that †-SCFAs in fdHilb canonically correspond to orthonormal bases (their unique basis of copyable, or *classical*, states), and can thus be used to model a basis of eigenstates; more generally, commutative †-Frobenius algebras (†-CFAs) correspond to orthogonal bases.

Strongly complementary pairs of classical structures appear in [10,11] to model non-locality in terms of commutative non-degenerate observables of generalized Mermin arguments. The paper [19] shows that they correspond to finite abelian groups in fdHilb and [15] specifies their connection to the Fourier Transform. The notion of phase groups was explicitly introduced in [10, 12]. Their connection to non-locality was first made in [12], where it was used to differentiate Spekkens toy theory from stabilizer quantum mechanics. Finally, the upcoming [8] and [17] provide a comprehensive reference for many structures and results used here. These, along with the survey [26], are also good references for the diagrammatic notation used throughout this literature.

3 Mermin measurements

Unlike Bell tests, which produce outcomes with probabilities that are forbidden to local hidden variable theories, the Mermin (or GHZ) argument produces outcomes which are impossible to observe in a local hidden variable theory [22]. This section introduces the definitions necessary to generalise the Mermin argument to abstract process theories. We make use of the standard definitions for strongly complementary observables, phase states and phases. We often refer to quasi-special †-Frobenius algebras as **non-degenerate observables** and use the shorthand †-qSFA. The acronym †-qSCFA refers to a commutative †-qSFA. Definitions of these concepts are reproduced in Appendix A.

Definition 3.1. A family $(|\psi_j\rangle)_j$ of states of an object $\mathscr{H}$ in a †-SMC forms a (orthogonal) **basis** if the following two conditions hold:

1. $\langle\psi_i|\psi_j\rangle = 0$ for $i \neq j$
2. for any $f, g : \mathscr{H} \to \mathscr{H}'$ we have that $\forall j.\ f|\psi_j\rangle = g|\psi_j\rangle$ implies $f = g$

In fdHilb, the objects are vector spaces and any orthogonal vector space basis clearly obeys these conditions. The above Definition allows us to extend the appropriate notion of a basis to an arbitrary †-SMC. Within the context of Categorical Quantum Mechanics, a †-qSCFA $\bullet$ with classical points forming a basis is said to have **enough classical points**. More details on phases and classical points of observables can be found in the Appendix.

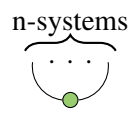
Theorem 3.2. *Let $\circ$ and $\bullet$ be strongly complementary †-qSFAs in any †-SMC. Phase states (resp. phases) of $\circ$ form group under the action of $(\text{⚲}, \text{⚲})$. This group of phase states is denoted the* **phase group** *$P_{\circ}$. The classical points (resp. the induced phases) of $\bullet$ are a subgroup $K_{\bullet} \subseteq P_{\circ}$.*

Proof. Proof that phases form a group can be found in [17]. Proof that classical points form a group can be found in [11] (for †-SCFAs) and [15]. Statement follows from this. □

When talking about the phase group of a †-qSCFA is commutative, we use additive notation: given two $\circ$-phase states $|\alpha\rangle$ and $|\beta\rangle$, we denote by $|\alpha+\beta\rangle$ their addition in the phase group. From now on, we interchangeably use phase states and phases, leaving disambiguation to context.

The GHZ states and Mermin measurements are the main ingredients needed in our argument. GHZ states appear in the ZX calculus fragment of our framework in [10] and are generalized to the definition that we use in [11].

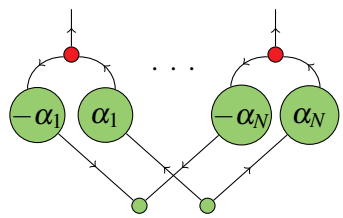
Definition 3.3. Given a †-qSFA ● in a †-SMC, an N**-partite GHZ state** for ● is:



(3.1)

Inspired by [11], we build Mermin type scenarios out of them.

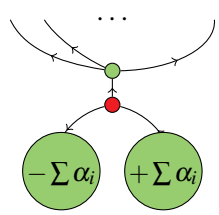
Definition 3.4. Let ● and ● be a pair of strongly complementary †-qSFAs in a †-SMC. An N-partite **Mermin measurement** is obtained by applying N ●-phases $\alpha_1, ..., \alpha_N$ to the N components of an N-partite GHZ state, and then measuring each component in the ● structure:



(3.2)

We further require that $\sum_i \alpha_i$, where the sum is taken in the group of phases, be a ●-classical point.

Lemma 3.5. *The Mermin measurement shown in Equation 3.2 is equivalent to the following state:*



(3.3)

Proof. Pushing the phases down through the ● nodes and using strong complementarity. See [11]. □

While this defines a single Mermin experiment, the full non-locality argument requires the joint outcomes of several Mermin measurements.

Definition 3.6. Let ● and ● be strongly complementary †-qSCFAs on a space $\mathscr{H}$ in a †-SMC. An N-partite **Mermin measurement scenario** (for ● and ●) is any non-empty, finite collection of Mermin measurements $\underline{\alpha}^s = (\alpha_1^s, ..., \alpha_N^s)_{s=1,...,S}$ of the N-partite GHZ state in the form of Equation 3.5.

In the category fdHilb of finite-dimensional Hilbert spaces, an N-partite Mermin measurement scenario where $a_1, ..., a_M$ are the distinct ●-phases appearing in the scenario and $\mathscr{H}$ is D-dimensional is exactly the usual (N, M, D) Mermin scenario. This correspondence is clarified in Section 4, where we derive our generalized Mermin non-locality argument.

4 Mermin locality and non-locality

The last definitions we need for our main results, Theorems 4.7 and 4.8, are those of local hidden variable models (following the construction of [11]) and non-trivial algebraic extensions.

Definition 4.1. Let $\bullet$ and $\bullet$ be strongly complementary †-qSCFAs on some system $\mathscr{H}$. Consider an N-partite Mermin measurement scenario $(\underline{\alpha}^s)_{s=1,\dots,S}$, and let $a_1,\dots,a_M$ be the distinct $\bullet$-phases appearing in it. The **local map** for the scenario is the map $\mathscr{H}^{\otimes(M\cdot N)} \to \mathscr{H}^{\otimes(N\cdot S)}$ defined as follows:

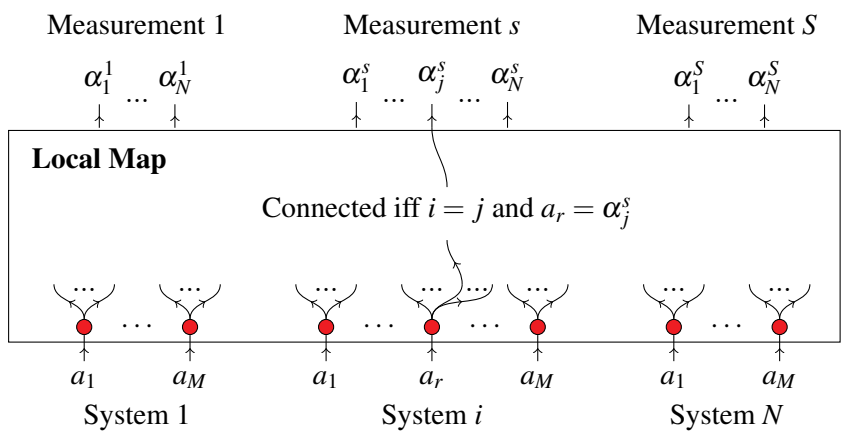
a. we group the input wires in N groups of M wires: we say that the r-th wire of i-th group is the a_r **input wire for system** i

b. we group the output wires in S groups of N wires: we say that the j-th wire of r-th group is the j-th **output wire for measurement** s

c. each input wire is connected to a $\bullet$ node

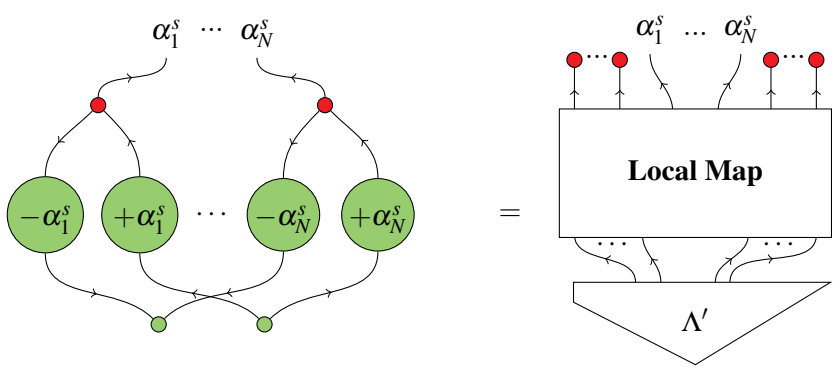
d. for all r,i,j and s, the $\bullet$ node of each a_r input wire for system i is connected to the j-th output wire for measurement s if and only if $i=j$ and $\alpha^s_j = a_r$

The following diagram details the procedure:



(4.1)

A **local hidden variable model** for an N-partite Mermin measurement scenario is a state Λ of $\mathscr{H}^{\otimes(N\cdot S)}$, obtained by applying the local map for the scenario to some state Λ' of $\mathscr{H}^{\otimes(M\cdot N)}$. We further require that for each $s=1,\dots,S$, the Mermin measurement $\underline{\alpha}^s$ is the same as the state obtained from Λ by composing an $\bullet$ with each output wires of each measurement t with $t\neq s$:



(4.2)

The definition of local hidden variables finally allows us to formulate our generalised notion of Mermin non-locality.

Definition 4.2. We say a †-SMC $\mathscr{C}$ is **Mermin non-local** if there exists a Mermin scenario for some strongly complementary pair $(\bullet,\bullet)$ of †-qSCFAs which has no local hidden variable model. If for all strongly complementary pairs no such measurement exists, then we say that $\mathscr{C}$ is **Mermin local**.

Mermin non-locality will shortly be shown to be equivalent to the following algebraic property of the group of $\bullet$-phases. The following examples will be used later on to investigate some abstract process theories of interest.

Definition 4.3. Let $(G,+,0)$ be an abelian group and $(H,+,0)$ be a subgroup. We say that G is a **non-trivial algebraic extension** of H if there exists a finite system of equations $(\sum_{j=1}^{l} n_j^p \cdot x_j = h^p)_p$, with $h^p \in H$ and $n_j^p \in \mathbb{Z}$, which has solutions in G but not in H. Otherwise, we say G is a **trivial algebraic extension** of H.

If $G = P_{\bullet}$ is a non-trivial algebraic extension of $H = K_{\bullet}$, then the $\bullet$-phases involved in any solution $x_j := \alpha_j$ to a system unsolvable in $K_{\bullet}$ will be called **algebraically non-trivial phases**.

Example 4.4. Let $G = \{0, \pi/2, \pi, -\pi/2\} < \mathbb{R}/2\pi\mathbb{Z}$ and $H = \{0, \pi\} < G$. Then G is a non-trivial algebraic extension of H, because the single equation $2x = \pi$ has no solution in H but has solution(s) $\pm\pi/2$ in G. It is in fact this example that yields the original argument in fdHilb from [11].

Lemma 4.5. *Let $(G,+,0)$ be an abelian group and $(H,+,0)$ be a subgroup. Suppose that there is a function $\Phi : G \to H$ such that for any equation $\sum_{j=1}^{l} n_j \cdot x_j = h$ with $h \in H$ and $n_j \in \mathbb{Z}$, if $x_j := g_j$ is a solution in G, $x_j := \Phi(g_j)$ is also a solution (in H). Then G is a trivial algebraic extension of H.*

Proof. Consider a system with solution $x_j := g_j$ in G. Then $x_j := \Phi(g_j)$ solves each individual equation in H, and thus also the system. □

Example 4.6. Let $(K,+,0)$ be any finite abelian group, and $G = K \times K'$ for some finite non-trivial abelian group $(K',+,0)$. Let $H < G$ be the subgroup $K \times \{0\}$. If $h = (k,0) \in H$, then any equation $\sum_{j=1}^{N} n_j \cdot x_j = h$ is equivalent to the following pair of equations, where π_K and $\pi_{K'}$ are the quotient projections onto $K \cong G/K'$ and $K' \cong G/K$ respectively:

a. $\sum_{j=1}^{N} n_j \cdot \pi_K x_j = k$ in K

b. $\sum_{j=1}^{N} n_j \cdot \pi_{K'} x_j = 0$ in K'

If $x_j := g_j = (\pi_K g_j, \pi_{K'} g_j)$ is a solution in G, then $x_j := (\pi_K g_j, 0)$ is a solution in H. Define Φ to be the map $g_j : G \mapsto (\pi_K g_j, 0) \in H$ and use Lemma 4.5 to conclude that G is a trivial algebraic extension of H.

We are now able to introduce our first main result:

Theorem 4.7 (Mermin Non-Locality)**.** *Let $\mathscr{C}$ be a †-SMC, and $(\bullet,\bullet)$ be a strongly complementary pair of †-qSCFAs. Suppose further that the $\bullet$-classical points form a basis. If the group of $\bullet$-phases is a non-trivial algebraic extension of the subgroup of $\bullet$-classical points, then $\mathscr{C}$ is Mermin non-local.*

Proof. For clarity, we present a proof where the system of equations that defines the phase group as a non-trivial algebraic extension is composed of a single equation. The construction for general systems of l equations consists of l copies of the construction we explicitly give.

Let $a_1, ..., a_M$ be $\bullet$-phases and $a \neq 0$ be (the phase induced by) a $\bullet$-classical point such that the following equation (in additive $\mathbb{Z}$-module notation, for $n_r \in \mathbb{Z}$) has solution $(x_r := a_r)_{r=1,...,M}$ in the group of $\bullet$-phases, but has no solution in the subgroup of (phases induced by) $\bullet$-classical points:

$$\sum_{r=1}^{M} n_r \cdot a_r = a \tag{4.3}$$

This means that we are assuming the group of $\bullet$-phases are a non-trivial algebraic extension of the subgroup of $\bullet$-classical points. Without loss of generality, assume that $n_r \neq 0$ and $a_r \neq 0$ for all $r = 1, ..., M$.

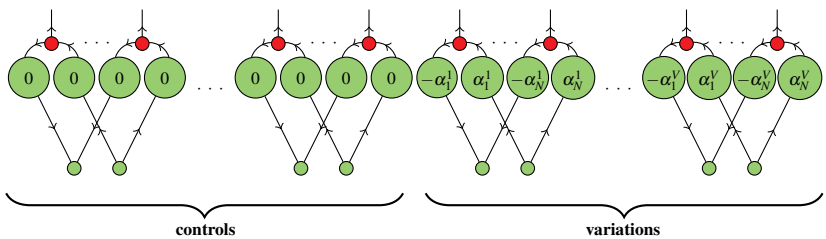
Let k be the exponent of the group of $\bullet$-classical points, and define the following Mermin measurement, where each a_r appears n_r times and 0 appears n_0 times, for some n_0 such that $V := \sum_{r=0}^{M} n_r \equiv 1 \pmod{k}$

$$\underline{\alpha} = (a_1, ..., a_1, ..., a_M, ..., a_M, 0, ..., 0) \tag{4.4}$$

Define a V-partite Mermin measurement scenario with $S := n_0 + V$ and:

$$\begin{aligned} \underline{\alpha}^s &:= (0, 0, ..., 0, 0) \text{ for } s = 1, ..., n_0 \\ \underline{\alpha}_i^{n_0+v} &:= \underline{\alpha}_{i+v \,(\mathrm{mod}\, V)} \text{ for } v = 1, ..., V \end{aligned} \tag{4.5}$$

The scenario has n_0 measurements with only 0 phases (the **controls**) and V measurements with cyclic permutations of $\underline{\alpha}$ (the **variations**). The following diagram depicts the scenario:



(4.6)

To show that the scenario from Equation 4.6 does not admit a local hidden variable:

1a. we add up (in the group of $\circ$-phases) all the components of each control, using Lemma 3.5, and obtain 0 from each control

1b. we add up all the components of each variation, again using Lemma 3.5, and obtain a from each variation

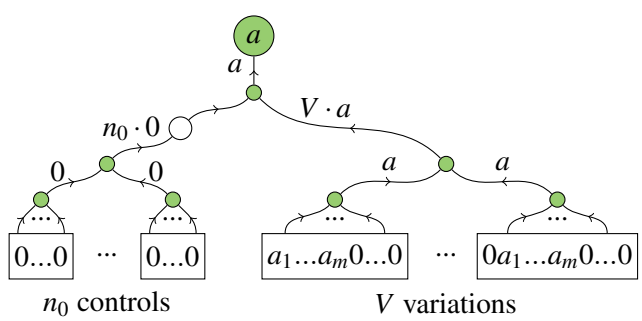
2a. we add up the result from all the controls, and obtain $\Sigma_C := n_0 \cdot 0 = 0$

2b. we add up the result from all variations, and obtain $\Sigma_V := V \cdot a = a$, using the fact that a is in the subgroup of (phases induced by) $\bullet$-classical points and V is congruent to 1 modulo the exponent of the subgroup

3. we subtract Σ_C from Σ_V, using the antipode ϕ of the strongly complementary pair ($\circ$,$\bullet$), and obtain $a - 0 = a$

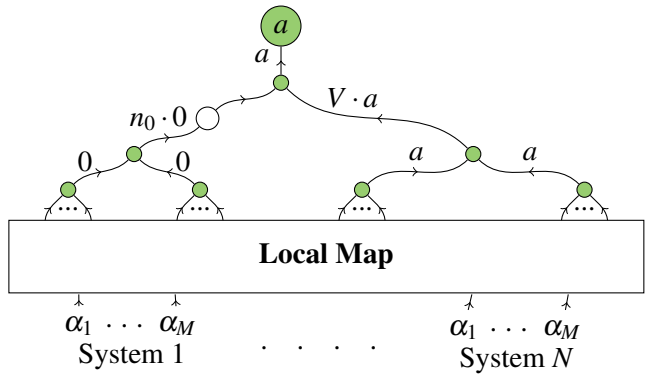
4. we test the result against the $\bullet$-classical point $\langle a|$, and obtain the non-zero scalar $\langle a|a\rangle$

The procedure is summarised by the following diagram:



(4.7)

The same procedure applied to any local hidden variable model always yields the 0 scalar. A local hidden variable model is nothing but the local map for the scenario applied to some state, so it is enough to show that the above procedure yields the constant 0 function when composed with the local map:

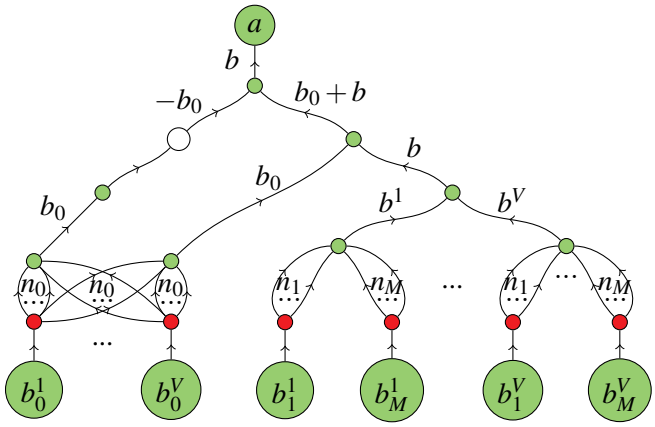


(4.8)

Since the ●-classical points form a basis, it is sufficient to show that the map from Diagram 4.8 always yields 0 when applied to ●-classical points. In the following diagram, the ● nodes have been re-arranged using the spider theorem, so that the wiring of the local map can be written down explicitly in a clean way. The diagram also annotates the ●-classical values on the wires at each stage to aid in following the argument:

1. the values $b_0^1, ..., b_0^V$ for the 0 phases of systems 1 to V are each duplicated $n_0 + n_0$ times and then added up to $b_0 := n_0 \cdot \sum i = 1^V b_0^i$ by the two ● nodes
2. the values $b_1^i, ..., b_m^i$ for the $a_1, ..., a_m$ phases of each system $i = 1$ (for $i = 1, ..., V$) are each duplicated n_k times (for $k = 1, ..., m$) and added up to $b^i := \sum_{r=1}^m n_r \cdot b_r^i$ by the respective ● nodes
3. the values $b^1, ..., b^V$ are added up to $b := \sum_{i=1}^V b^i$
4. the value b_0 is added up to b
5. finally, the value b_0 is subtracted from b, and b is tested against the ●-classical point $\langle a|$, obtaining the scalar $\langle a|b\rangle$ (which we want to be zero)

The steps are summarised by the following diagram:



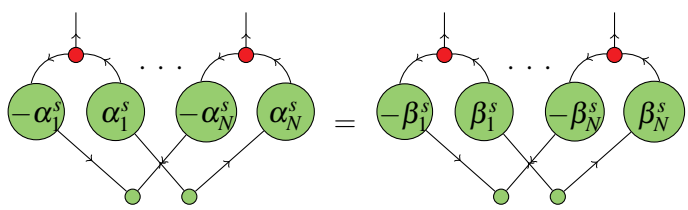
(4.9)

The ●-classical points c that can be written as $c = \sum_{r=1}^M n_r \cdot c_r$ for some ●-classical points $c_1, ..., c_M$ form a subgroup H of the group of ●-classical points. Indeed we have that $0 = \sum_{r=1}^m n_r \cdot 0$ and that

$(\sum_{r=1}^{M} n_r \cdot c_r) + (\sum_{r=1}^{M} n_r \cdot d_r) = \sum_{r=1}^{M} n_r \cdot (c_r + d_r)$. Furthermore, by assumption we have that H does not contain a, and as a consequence $\langle a|c\rangle = 0$ for all $c \in H$. Going back to Diagram 4.9, we see that $b^1, ..., b^V \in H$ (but b_0 need not be in H, hence the need to subtract it before testing against a). We thus conclude that $b \in H$ (since H is closed under addition): hence the scalar $\langle a|b\rangle$ vanishes, concluding our proof that no local hidden variable can exist for our chosen measurement scenario. □

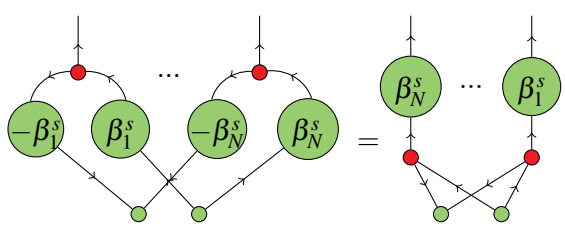
Theorem 4.8 (Mermin Locality)**.** *Let $\mathscr{C}$ be a †-SMC. If for any strongly complementary pair $(\circ, \bullet)$ of †-qSCFAs the group of $\circ$-phases is a trivial algebraic extension of the subgroup of $\bullet$-classical points (i.e. if there exist no algebraically non-trivial $\circ$-phases), then $\mathscr{C}$ is Mermin local.*

Proof. Consider an N-partite Mermin measurement scenario $\underline{\alpha}^s = (\alpha_1^s, ..., \alpha_N^s)_{s=1,...,S}$, and let $a_1, ..., a_M$ be the distinct $\circ$-phases appearing in it. Consider the system of equations $(\sum_{r=1}^{M} n_r^s \cdot x_r = c^s)_{s=1,...,S}$, where n_r^s is the numer of times phase a_r appears in measurement $\underline{\alpha}^s$, and c^s are the unique values making $x_r := a_r$ into a solution for the system. As the group of $\circ$-phases is a trivial algebraic extension of the subgroup of $\bullet$-classical points, there is a solution $x_r := b_r$ with $(b_r)_{r=1,...,M}$ $\bullet$-classical points. By using this, together with Lemma 3.5, we see that each measurement in the scenario is equal to the Mermin measurement obtained by replacing a_r with b_r for all $r = 1, ..., M$ (say $\beta_i^s := b_r$ if $\alpha_i^s = a_r$):



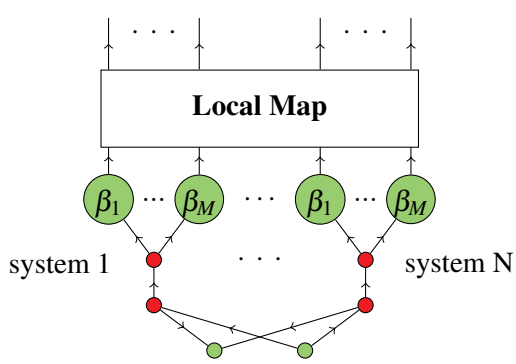
(4.10)

All phases are now induced by $\bullet$-classical points, and can thus be pushed up through the s:



(4.11)

Now that each measurement of the scenario amounts to performing some set of $\bullet$-classical operations on the same state, it is no surprise that the following gives a local hidden variable model:



(4.12)

□

The abstract framework can now be applied to some particular examples of interest.

Corollary 4.9. *The restricted ZX calculus (that corresponds to qubit stabilizer quantum mechanics) from [4, 10] (referred to as Stab in [11]) is Mermin non-local.*

Proof. Take $\bullet$ and $\bullet$ to be the Z and X single-qubit observables in the ZX calculus. The group of $\bullet$-phases is $\mathbb{Z}_4$ and the subgroup of $\bullet$-classical points is $\mathbb{Z}_2$. Conclude with Theorem 4.7 and Example 4.4. □

Corollary 4.10. *The toy theory Spekk from [11] is Mermin local.*

Proof. Same setup as in the previous corollary, but the phase group is now $\mathbb{Z}_2 \times \mathbb{Z}_2$. Conclude using Theorem 4.8 and Example 4.6 with $d = 2$. □

Corollary 4.11. *Qutrit stabilizer quantum mechanics from [24] is Mermin local.*

Proof. The phase group here is $\mathbb{Z}_3 \times \mathbb{Z}_3$. Conclude using Theorem 4.8 and Example 4.6 with $d = 3$.[1] □

Corollary 4.12. *The category* fRel *of finite sets and relations is Mermin local.*

Proof. See [15, 17] for more details on strong complementarity in fRel. Any †-qSCFA on a set $\mathscr{H}$ in fRel is a groupoid: we write it in the form $\oplus_{h\in H} G_h$, where H is a set, G_h are disjoint groups and $\cup_{h\in H} G_h = \mathscr{H}$. Any strongly complementary pair $\bullet, \bullet$ is in the form $(\oplus_{h\in H} G, \oplus_{g\in G} H)$, where both G and H are groups (seen as sets when indexing the groupoids), and we can w.l.o.g. write $\mathscr{H}$ as $G \times H$. Each $\bullet$-classical points is in the form $\{(g,h) \text{ s.t. } h \in H\}$ for some $g \in G$, while the $\bullet$-phases are in the form $\{(g_h, h) \text{ s.t. } h \in H\}$, for some family $(g_h)_{h\in H}$ of elements of G. Thus the group of $\bullet$-phases is the group G^H of H-indexed vectors with values in G, and the subgroup of $\bullet$-classical points, isomorphic to G, is that of vectors with constant components. Conclude using Theorem 4.8 and Example 4.6. □

This last result is particularly interesting for the following reasons:

1. Almost no †-qSCFAs in fRel have enough classical points (exactly one per space, out of a number that grows exponentially with space size).
2. The family of arguments from [11] fails in fRel (partially as a consequence of the previous point).
3. There are plenty of strongly complementary pairs in fRel, and arbitrarily many more $\bullet$-phases than $\bullet$ classical points, but the lack of *algebraically non-trivial* phases results in fRel being Mermin local.
4. As a consequence of point 3, quantum protocols relying only on Mermin non-locality will show no quantum advantage in fRel.

[1] This example was first constructed by Edwards in [12] without reference to the qutrit stabilizer formalism. This work also anticipated Example 4.6, using a specific construction.

5 Mermin in fdHilb: beyond the complementary XY pair

We now focus on fdHilb and quantum mechanics. While in general we can have many different choices of measurement on each subsystem (see Definition 3.4), we shall restrict to the case of only two distinct measurements, i.e. $(N, M = 2, D)$ scenarios. In the case of qubits and $(N, 2, 2)$ scenarios, these complementary measurements happen to be the only choices that will lead to a non-locality argument. One might then conjecture that this will be the case for any dimension. In this section we show that this assumption is not the case. For $(N, 2, D)$ scenarios it is not necessary to have the two measurements be complementary. There are many possible pairs in general.

Definition 5.1. A **two-measurement Mermin scenario** for N systems (each with D dimensions) and strongly complementary GHZ observable with $\bullet$-phase group G is denoted $G(N, 2, D)$. Each system has two possible measurement settings:

1. the first measurement observable is the D-dimensional X observable,
2. and the second measurement observable B is defined by a Z-phase gate applied to X.

In general, the form of B can be specified by the D-dimensional Z-phase applied to X. This Z-phase is of the form $(1, e^{1b_1}, ..., e^{ib_{D-1}})^T$ with $D-1$ degrees of freedom. A two-measurement Mermin scenario thus consists of V variations each with β measurements of the B observable.

Example 5.2. For qubits there is only a single possible phase group: $\mathbb{Z}_2$. A Mermin argument for three qubits (denoted $\mathbb{Z}_2(3, 2, 2)$) has measurements of the usual X observable and of the B observable that is a phase applied to X, i.e. $\mathrm{diag}(1, e^{ib_1})X$. In the traditional Mermin scenario $\mathbb{Z}_2(3, 2, 2)$ from [22], we have $V = 3$ and $\beta = 2$.

The state presented in Diagram 4.9 will be zero when the *control point* on the left is distinct from the *variations point* on the right. We can characterize this as a condition on B in our two measurement scenario with the following theorem.

Lemma 5.3. *Measurements X and B allow a $(N, 2, D)$ Mermin non-locality argument iff*

$$\sum_{j=1}^{D-1} e^{ic_j} = -1, \qquad \text{where } c_j = b_j \left(\bigoplus_{i=1}^{V} \beta \right), \tag{5.1}$$

where the sum in c_j is the group sum for the $\bullet$-phase group G.

Proof. Diagram 4.9 implies that the Mermin argument will succeed when the control point and variations point are distinct classical points. In fdHilb this precisely means that they are orthogonal vectors. The vector that represents the control point is given by the D-dimensional unit for the X observable, i.e. $1/\sqrt{D}(1, 1, ..., 1)^T$. The variations point is then given by the group sum of other classical points specified by their phase. The phase for each classical point is given by the sum of phase accumulated by each B measurement. As there are β such measurements in each variation, their sum is given by

$$\frac{1}{\sqrt{D}} \begin{pmatrix} 1 \\ e^{i\beta b_1} \\ \vdots \\ e^{i\beta b_{D-1}} \end{pmatrix}_1 \oplus \begin{pmatrix} 1 \\ e^{i\beta b_1} \\ \vdots \\ e^{i\beta b_{D-1}} \end{pmatrix}_2 \oplus ... \oplus \begin{pmatrix} 1 \\ e^{i\beta b_1} \\ \vdots \\ e^{i\beta b_{D-1}} \end{pmatrix}_V = \frac{1}{\sqrt{D}} \begin{pmatrix} 1 \\ e^{ic_1} \\ \vdots \\ e^{ic_{D-1}} \end{pmatrix},$$

where the constants c_j are defined as in Equation 5.1. Orthogonality between the control and variations points then requires

$$\begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 \\ e^{ic_1} \\ \vdots \\ e^{ic_{D-1}} \end{pmatrix} = 0 \qquad \Rightarrow \qquad \sum_{j=1}^{D-1} e^{ic_j} = -1$$

This exactly recovers Equation 5.1 and completes the proof. □

This gives a necessary and sufficient condition on these measurements to enable a Mermin non-locality test. Note that in Mermin's original scenario measurement observables were necessarily complementary, but that in general this is not the case.

Theorem 5.4. *In* $(3,2,2)$ *three qubit Mermin scenarios, the two measurements must be complementary.*

Proof. We have $V = 3$, $\beta = 2$, $G = \mathbb{Z}_2$ and $D = 2$. Thus

$$c_j = \beta b_j \left(\bigoplus_{l=1}^{3} 1 \right) = 2b_j(3 \mod 2) = 2b_j$$

so that our condition on B becomes

$$\sum_{j=1}^{D-1} e^{ic_j} = e^{i2b_1} = -1 \Rightarrow b_1 = \frac{\pi}{2}$$

with only a single solution. This means that in this scenario there is only one measurement that could be used with X. This is the Y observable and it is complementary to X. □

Theorem 5.5. *For* $(N,2,D)$ *scenarios the measurements need not be complementary.*

Proof. We prove this by counterexample. Consider the three dimensional ($D = 3$) five party Mermin scenario. The phase group of the non-local state is then given by $G = \mathbb{Z}_3$. The control measurement is given by five systems all measured by the X observable, i.e. XXXXX. The variations are

$$\begin{array}{ccccc} BBBXX & BBXBX & BXBBX & XBBBX & XBXBB \\ BBXXB & BXBXB & XBBXB & BXXBB & XXBBB \end{array}$$

so that $V = 10$ and $\beta = 3$. We calculate the coefficients

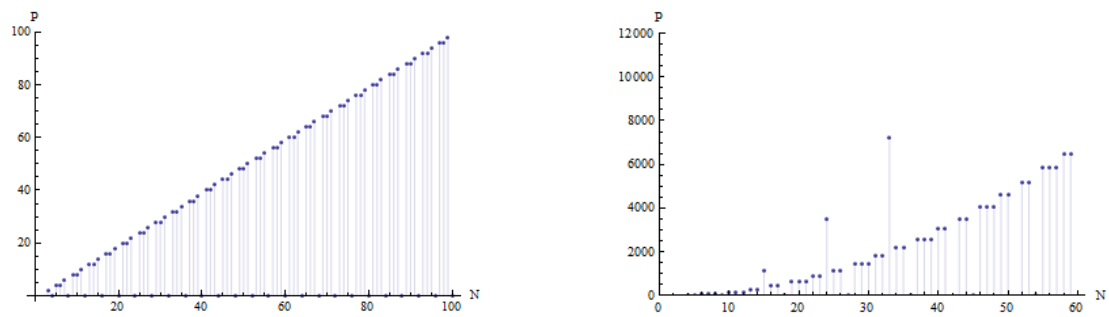
$$c_j = \beta b_j \left(\bigoplus_{l=1}^{10} 1 \right) = 3b_j(10 \mod 3) = 3b_j$$

Observable B must then satisfy $e^{i3b_1} + e^{i3b_2} = -1$. Any B observable satisfies this condition if $b_2 = -\frac{i}{3}\log\left[-1 - e^{3ib_1}\right]$. Consider $b_1 = \frac{2\pi}{9} \Rightarrow b_2 = -\frac{2\pi}{9}$ and calculate (for $\omega = e^{2\pi i/3}$):

$$B :: \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i2\pi/9} & 0 \\ 0 & 0 & e^{-i2\pi/9} \end{pmatrix} \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ e^{2i\pi/9} & e^{8i\pi/9} & e^{-4i\pi/9} \\ e^{-2i\pi/9} & e^{-8i\pi/9} & e^{4i\pi/4} \end{pmatrix}$$

Observable B is clearly not complementary to X by simply checking the dot products of their basis vectors. □

Further we can exhibit numerical results that calculate the number of Mermin effective measurement pairs available for a particular scenario. For a given number of parties N we have calculated the number of effective pairs maximized over all viable variation choices. Typically these maximum values are found for variations where β is maximized. Figure 1a shows pair counts for $\mathbb{Z}_2(N,2,2)$ scenarios. Here is appears that the number of effective measurement pairings grows approximately linearly with the number of parties. Figure 1b shows pair counts for the more complex $\mathbb{Z}_3(N,2,3)$ scenarios. It is clear that there are many (in some cases thousands) more available measurement configurations than just those given by complementary observables. This vastly expands the number of experimental setups that will generate, with certainty, a non-locality violation. Indeed, combining this result with those of Section 6 opens up a large class of quantum secret sharing protocols based on non-complementary measurements.



(a) (b)

Figure 1: (a) A plot of the number of Mermin effective measurement pairs P vs. the number of parties in the Mermin scenario N for $\mathbb{Z}_2(N,2,2)$ scenarios. (b) A plot of the number of effective pairs for $\mathbb{Z}_3(N,2,3)$ scenarios. These numbers were obtained by numerically counting solutions to (5.1).

6 Quantum Secret Sharing: non-locality as a resource

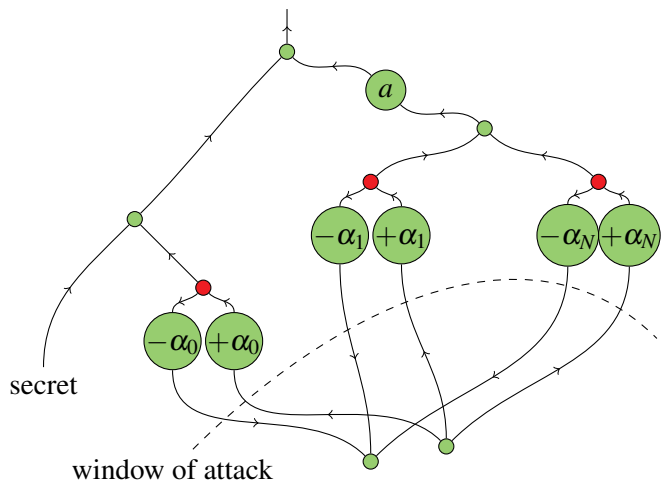
The HBB CQ (N,N) family of Quantum Secret Sharing protocols originates in [20, 21], and has been abstractly formulated in Categorical Quantum Mechanics [28]. Here we generalise their construction to abstract process theories, unearthing a deep connection with Mermin non-locality.

This protocol requires a pair $(\bullet,\bullet)$ of strongly complementary observables, and an $(N+1)$-partite GHZ state shared by the dealer and the N players. The dealer (and nobody else) knows the (classical) secret, in the form of a $\bullet$-classical point. The aim of the protocol is for the dealer to broadcast some information to all players on a public classical channel, and for the secret to be deterministically decodeable if only if all N players cooperate. The implementation, graphically summarised in 6.1, goes as follows:

1. the dealer and the players agree on a random set of $\bullet$-phases $\alpha_0, \alpha_1, \ldots, \alpha_N$ such that $\sum \alpha_j$ is some $\bullet$-classical point (call it a). This operation is done on a public channel.
2. the dealer measures his part of the system of the system with phase α_0, and uses the resulting $\bullet$-classical data to encode the plaintext secret (classically adding the secret and the measurement data in the group $K_\bullet$; this generalises the original XOR operation, corresponding to $K_\bullet = \mathbb{Z}_2$ with addition mod 2) into a classical cyphertext. This operation is done locally and privately by the dealer.
3. the dealer broadcasts the cyphertext on a public classical channel to the players.

4. at some later stage, when they all agree to unveil the secret, the N players measure their part of the system, each locally and privately.
5. all players broadcast the $\bullet$-classical results of their measurements on a public classical channel.
6. the broadcast results can be classically added in $K_\bullet$, then the result can be added to a and finally to the cyphertext (again in the group $K_\bullet$) to recover the original $\bullet$-classical plaintext secret.

(6.1)



Most of the operations are either done locally and privately (all the measurements and the secret encoding), or broadcast by design on public classical channels, where one assumes that integrity of the message is guaranteed by appropriate classical protocols. There are many additional layers of quantum guarantees coming with this protocol, depending on the level of tampering allowed and on the phases chosen:

1. Assume no tampering happens anywhere. Then the refusal of (at least) one player to broadcast his or her measurement result makes the secret totally random to anyone else.
2. Assume that an attacker is allowed to tamper *only* with the GHZ state, and *before* the phases are chosen. Then the maximum amount of information she can gain is limited by (a) the random distribution on phases and (b) the amount of bias between the possible phases for each system. If p_{max} is the highest probability appearing in the distribution of the phase choices (traditionally uniform with probability $1/^N$)[2], and we let $k := |K_\bullet|$ be the dimensionality of the space (traditionally $k = 2$ for qubits), then optimal tampering reveals an average of p_{max} k-its of classical information (on a secret of 1 k-it), in the case where the alternative measurements on each system are mutually unbiased (e.g. the traditional X, Y pair). A more complicated failure expression can be worked out for arbitrary bases. This gain in information, however, is compensated by the introduction of a probability of failure for the entire protocol of $(1 - p_{max}) \cdot (1 - 1/k)$ (again in the mutually unbiased case), which can be detected by the players/dealer via statistical analysis of the outcomes.
3. The kind of tampering allowed in the previous point does not give significant advantage to the attacker (at least for large number of players), and can be mitigated by appropriate statistical analysis of the measurement outputs; however, there is a stronger form of tampering that we can consider. Assume that the attacker is allowed to tamper with the GHZ state after the phases have been chosen, or even with the measurement devices of the dealer/player themselves, in a way that will

[2]Not $1/2^{N+1}$, because of the parity requirement.

ensure he knows the measurement outcomes with certainty beforehand; this is the model of attack assumed by device-independent security, pioneered in [5]. Under this stronger model of attack, we can show that the protocol is secure if and only if the phases chosen by the players are algebraically non-trivial. Indeed, from the point of view of the dealer/players, the attack results in the measurement outcomes having a classical probability distribution:

(a) if the phases are algebraically non-trivial, the probability distribution in the tampered case will never match, because of contextuality, that generated by the un-tampered protocol, and the attack can be detected by statistical analysis of the outcomes.

(b) if the phases are algebraically trivial, on the other hand, they admit a probabilistic local hidden variable, and the attacker can generate her deterministic outcomes in a way to mimic the probability distribution of the un-tampered protocol.

To summarise, there are three distinct quantum resources playing complementary roles in the security of this protocol: the entanglement structure of the GHZ state, the amount of mutual complementarity of the available phases, and their algebraic non-triviality. Firstly, the entanglement structure of the GHZ state is the resource ensuring that the refusal of one player to cooperate results, if no tampering is allowed, into the inability for everyone else to recover the secret. Secondly, the amount of mutual complementarity of the available phases, e.g. the complementarity of the X, Y pair, limits the maximum amount of information an attacker can gain by tampering with the state before phases are chose, and the minimum amount of disturbance introduced by the attack. Finally, Mermin non-locality, or equivalently algebraic non-triviality of the chosen phases, is the key resource ensuring device-independent security of the protocol.

7 Conclusions and future work

By using few, simple ingredients — †-SMCs, strongly complementary pairs, GHZ states, phases and classical points — we have generalised Mermin measurements to arbitrary abstract process theories. We have defined Mermin non-locality, and we have proven that a necessary and sufficient[3] condition for it is the existence of algebraically non-trivial phases, i.e. of phases which satisfy equations that classical points cannot. As a corollary, we have confirmed the well-known result that the stabilizer ZX calculus (and therefore fdHilb) is Mermin non-local, and we have proven that fRel, a toy category of choice for Categorical Quantum Mechanics, is Mermin local (despite its unboundedly large ratio of phases to classical points). This characterisation as the existence of certain phases opens the way to the treatment of Mermin non-locality as a resource in the abstract design of quantum protocols, as we have exemplified with the HBB CQ family of Quantum Secret Sharing protocols. Finally, the application of our general framework to Mermin-type experiment in quantum mechanics allows us to show that, even in the restricted case of two-measurement scenarios, complementary measurements are not necessary, leading to many more potential configurations than previously believed. We conclude with a few open questions for investigation:

1. What are the minimal conditions under which algebraically non-trivial phases lead to non-locality?
2. What is the exact connection between this framework as the framework of Abramsky et al. [1] for generalised All-versus-Nothing arguments where measurement outcomes are elements of some general field?

[3] Always necessary, sufficient under the assumption that classical points form a basis.

3. Is there a more informative group-theoretic formulation of the algebraic non-triviality used here?
4. Our analysis focuses on non-locality paradoxes for a kind of GHZ state. It was recently shown by [27] that multipartite non-locality arguments can be constructed from any of a set of qudit graph states that they call GHZ graphs. What are the connections between these qudit graph states and the phase group formalism we present here?
5. Which other quantum algorithms depend on Mermin non-locality as a resource to transcend classicality? Which process theories show these characteristics?

Acknowledgements The authors would like to thank Bob Coecke and Aleks Kissinger for plenty of comments and suggestions, as well as Sukrita Chatterji and Nicolò Chiappori for useful discussions and support. Funding from EPSRC (award number OUCL/2013/SG) and Trinity College for the first author and the Rhodes Trust and AFOSR grant FA9550-14-1-0079 for the second is gratefully acknowledged. Both authors contributed equally to this work.

References

[1] Samson Abramsky, Rui Soares Barbosa, Kohei Kishida, Raymond Lal & Shane Mansfield (2015): *Contextuality, Cohomology and Paradox*. arXiv preprint arXiv:1502.03097.

[2] Samson Abramsky & Adam Brandenburger (2011): *The sheaf-theoretic structure of non-locality and contextuality*. New Journal of Physics 13(11), p. 113036, doi:10.1088/1367-2630/13/11/113036.

[3] Samson Abramsky & Bob Coecke (2008): *Categorical quantum mechanics*. Handbook of quantum logic and quantum structures: quantum logic, pp. 261–324, doi:10.1016/B978-0-444-52869-8.50010-4.

[4] Miriam Backens (2014): *The ZX-calculus is complete for stabilizer quantum mechanics*. New Journal of Physics 16(9), p. 093021, doi:10.1088/1367-2630/16/9/093021.

[5] J. Barrett, L. Hardy & A. Kent (2005): *No signaling and quantum key distribution*. Phys. Rev. Lett. doi:10.1103/PhysRevLett.95.010503.

[6] Jonathan Barrett (2007): *Information processing in generalized probabilistic theories*. Physical Review A 75(3), p. 032304, doi:10.1103/PhysRevA.75.032304.

[7] J. S. Bell (1964): *On the Einstein-Podolsky-Rosen paradox*. Physics 1, pp. 195–200.

[8] B. Coecke & A. Kissinger (2015 (to appear)): *Picturing Quantum Processes*. Cambridge University Press.

[9] B. Coecke, E. O. Paquette & D. Pavlovic (2008): *Classical and quantum structuralism*. Semantic techniques for quantum computation, p. 43. Available at `http://arxiv.org/abs/0904.1997`, doi:10.1017/CBO9781139193313.003.

[10] Bob Coecke & Ross Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. New Journal of Physics 13(4), p. 043016, doi:10.1088/1367-2630/13/4/043016.

[11] Bob Coecke, Ross Duncan, Aleks Kissinger & Quanlong Wang (2012): *Strong complementarity and non-locality in categorical quantum mechanics*. In: Proceedings of the 2012 27th Annual IEEE/ACM Symposium on Logic in Computer Science, IEEE Computer Society, pp. 245–254, doi:10.1109/LICS.2012.35.

[12] Bob Coecke, Bill Edwards & Robert W Spekkens (2011): *Phase groups and the origin of non-locality for qubits*. Electronic Notes in Theoretical Computer Science 270(2), pp. 15–36, doi:10.1016/j.entcs.2011.01.021.

[13] Bob Coecke, Dusko Pavlovic & Jamie Vicary (2013): *A new description of orthogonal bases*. Mathematical Structures in Computer Science 23(03), pp. 555–567, doi:10.1017/S0960129512000047.

[14] Artur K. Ekert (1991): *Quantum cryptography based on Bell's theorem*. Phys. Rev. Lett. 67, pp. 661–663, doi:10.1103/PhysRevLett.67.661.

[15] S. Gogioso & W. Zeng (2015): *Fourier transforms from strongly complementary observables*. arXiv preprint arXiv:1501.04995.

[16] Stefano Gogioso (2015): *Categorical Semantics for Schrodigner's Equation*. arXiv preprint arXiv:1501.06489.

[17] C. Heunen & J. Vicary (2015 (to appear)): *Categories for Quantum Theory : An Introduction*.

[18] Seung-Woo Lee Jinhyoung Lee & M. S. Kim (2006): *Greenberger-Horne-Zeilinger nonlocality in arbitrary even dimensions*. Physical Review A 73. Available at `arXiv:quant-ph/0408072`, doi:10.1103/PhysRevA.73.032316.

[19] A. Kissinger (2012): *Pictures of Processes: Automated Graph Rewriting for Monoidal Categories and Applications to Quantum Computing*. Ph.D. thesis. Available at `http://arxiv.org/abs/1203.0202`.

[20] F-G. Deng L. Xiao, G. L. Long & J-W Pan (2004): *Efficient multiparty quantum-secret-sharing schemes*. Physical Review A, doi:10.1103/PhysRevA.69.052307.

[21] V. Buzek M. Hillery & A. Berthiaume (1999): *Quantum Secret Sharing*. Physical Review A, doi:10.1103/PhysRevA.59.1829.

[22] N David Mermin (1990): *Quantum mysteries revisited*. Am. J. Phys 58(8), pp. 731–734, doi:10.1119/1.16503.

[23] Serge Massar Nicolas Cerf & Stefano Pironio (2002): *Greenberger-Horne-Zeilinger paradoxes for many qudits*. Physical Review Letters 89. Available at `arXiv:quant-ph/0107031`, doi:10.1103/PhysRevLett.110.100403.

[24] André Ranchin (2014): *Depicting qudit quantum mechanics and mutually unbiased qudit theories*. arXiv preprint arXiv:1404.1288, doi:10.4204/EPTCS.172.6.

[25] Junghee Ryu, Changhyoup Lee, Zhi Yin, Ramij Rahaman, Dimitris G Angelakis, Jinhyoung Lee & Marek Żukowski (2014): *Multisetting Greenberger-Horne-Zeilinger theorem*. Physical Review A 89(2), p. 024103, doi:10.1103/PhysRevA.89.024103.

[26] Peter Selinger (2011): *A survey of graphical languages for monoidal categories*. In: *New structures for physics*, Springer, pp. 289–355, doi:10.1007/978-3-642-12821-94.

[27] Weidong Tang, Sixia Yu & CH Oh (2013): *Greenberger-Horne-Zeilinger paradoxes from qudit graph states*. Physical review letters 110(10), p. 100403, doi:10.1103/PhysRevLett.110.100403.

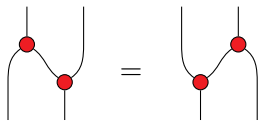
[28] V. N. Zamdzhiev (2012): *An Abstract Approach towards Quantum Secret Sharing*. Available at `http://www.cs.ox.ac.uk/people/bob.coecke/VladimirZamdzhievThesis.pdf`.

[29] M. Zukowski & D. Kaszlikowski (1999): *Greenberger-Horne-Zeilinger paradoxes with symmetric multiport beam splitters*. Physical Review A. Available at `arxiv:quant-ph/9911039`, doi:10.1103/PhysRevA.59.3200.

A Preliminary definitions

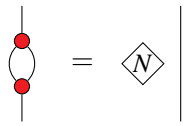
In this section we recall some basic background definitions from the literature [10]. We will use the diagrammatic language of symmetric monoidal categories, c.f. [26].

Definition A.1. In a †-symmetric monoidal category (†-SMC), the pair of a monoid (A, μ, η) and comonoid (A, δ, ϵ) form a **dagger-Frobenius algebra** (or †-FA) when the following equation holds:



(A.1)

Definition A.2. A **quasi-special** †-Frobenius algebra (, , ,) in a †-SMC is a Frobenius algebra that satisfies:



(A.2)

for some invertible scalar N.

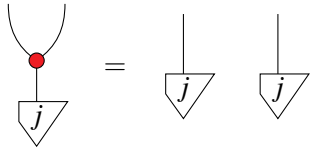
These †-qsFA are **commutative** when the monoid and comonid are commutative.

Theorem A.3 ([13, Thm 5.1])**.** *Commutative dagger Frobenius algebras in* fdHilb *are orthogonal bases.*

The additional condition of specialness (quasi-specialness where $N = 1$) for †-qsCFA acts as a normalizing condition so that:

Theorem A.4 ([13, Sec 6])**.** *Commutative dagger Frobenius algebras in* fdHilb *in* fdHilb *are orthonormal bases.*

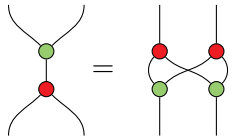
Definition A.5. The set of **classical states** K for a †-Frobenius algebra $(A, , , ,)$ are all states $j : I \to A$ such that:



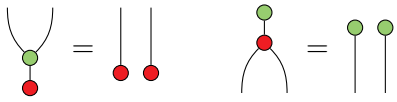
(A.3)

We now define strong complementarity, the first fundamental ingredient of Mermin measurements.

Definition A.6. A pair of †-qSFAs (, , ,) and (, , ,) is **strongly complementary** if it satisfies the following **bialgebra equation** (A.4) and **coherence equations** (A.5):



(A.4)



(A.5)

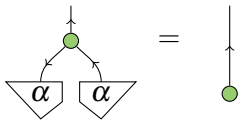
From now on we shall refer to the structures by their colour, i.e. by and . A more familiar presentation of strongly complementary pairs can be given by observing that they correspond (when both structures have enough classical points to form a basis) to pairs of non-degenerate observables obeying the finite-dimensional Weyl form of the Canonical Commutation Relations [16]. Also, we have the following characterisation of strong complementarity in terms of group actions on classical points.

Theorem A.7. *Let and be a pair of †-qSFAs. If the pair is strongly complementary, then (,) acts as a group on the classical points of . We denote this group as K. Conversely, if the -classical points form a basis and (,) acts as a group on them, then the pair is strongly complementary.*

Proof. See [15]. □

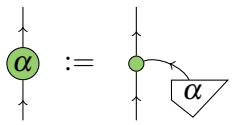
Phases are the other fundamental ingredient of Mermin measurements.

Definition A.8. A **phase state** for a †-qSCFA $\bullet$ is a pure state $|\alpha\rangle$ such that:



(A.6)

A **phase** is a map in the following form, where $|\alpha\rangle$ is a phase state for $(\bullet)$:



(A.7)

In particular, elements of $K_{\bullet}$ are phase states, as Theorem 3.2 explains.