Non-locality in Categorical Quantum Mechanics

William Edwards
Wolfson College, Oxford

Oxford University Computing Laboratory

Submitted for the degree of Doctor of Philosophy
Michaelmas Term 2009

Abstract

Interest has grown in recent years in the construction of 'quantum-like' theories, toy theories which exhibit some but not all features of quantum mechanics. Such theories are expressed in diverse mathematical terms which may impede comparison of their properties. In this thesis we present a unifying mathematical framework in which we can compare a variety of 'quantum-like' theories, based on Abramsky and Coecke's work on applying category theory to quantum mechanics. By doing so we hope to gain a clearer insight into the precise ways in which these theories differ mathematically, and whether this relates to the differences in phenomena which they predict. As an example of this kind of approach, we express Spekkens's toy bit theory within the categorical framework, in the process proving its consistency. The toy bit theory reproduces many features of quantum mechanics, and this is reflected in the fact that within the categorical framework it shares many structural features with quantum mechanics. It differs however, in that it is, by construction, a local hidden variable theory. We develop a categorical treatment of hidden variables, and then demonstrate that the categorical structures which differ between quantum mechanics and the toy theory are exactly those which relate to the question of hidden variables. We extend this to a general result applying to a wider range of theories.

Acknowledgements

I was fortunate to have not one but two excellent supervisors throughout my time at Oxford, Samson Abramsky and Bob Coecke. They were both extremely generous with their time, making themselves available to talk to and assist me to an extent which would be the envy of most doctoral students. They also made it possible for me to travel to conferences and meet prominent researchers in the field to a degree far beyond anything that most DPhil students could expect. Inspirational yet approachable they were an invaluable aid to me in completing this thesis.

I benefited greatly from discussions with many colleagues, both established researchers and fellow DPhil students. Particular mention should go to Rob Spekkens, and to Ross Duncan, Ben Jackson and Colin Stephen.

My parents have given me phenomenal support (both emotional and material!) throughout my protracted period in education. I'm extremely grateful to them, and the knowledge that they are always there when I need them is a great comfort to me. Without their help there is no way I would be where I am today. There would also be a large number of spelling mistakes in this thesis.

I was supported throughout my DPhil by an EPSRC studentship awarded by Oxford University Computing Laboratory, without which it would have been impossible to complete this work. I'm grateful to the Comlab for welcoming a physicist and giving me a good home for four years! I even learned a little bit about computers. Wolfson College provided me with an excellent base, a beautiful place to live, and a welcoming society of fellow students and researchers. The collegiate system at Oxford is an excellent means for academics to meet people from outside of their field, and Wolfson did an excellent job of continuing this tradition.

This thesis is dedicated to two people who sadly didn't live to see it finished: my grandfather Brian Thomas, and my best friend Ian 'Lenny' Linington. My grandfather had a great interest in science and a great respect for scientists, and it was he who first inspired my interest in physics. He continually encouraged me in my studies, and I'm very sad that he wasn't able to see me complete them. I first met Lenny while we were supervision partners studying physics at Cambridge. We both had a deep interest in the fundamental questions of the subject, and I probably learned more from my discussions with him than from any of the courses I took! I look back fondly on our many adventures together. He had recently completed a PhD himself, and had made very successful progress in his research career before it was halted tragically early. I miss them both very much.

Contents

Chapter 1

Introduction

Quantum mechanics has many distinctive features which diverge from traditional classical theories. Observable properties of systems and their measurements are treated in a radically different way. Most states have no definite value for each observable, instead existing as 'superpositions'. Certain pairs of observables are 'incompatible' and cannot be simultaneously measured. Composite systems can exist in 'entangled' states which cannot be specified simply by describing the state of each component. Quantum states cannot be cloned. And quantum states and processes allow information processing protocols to be performed which are impossible with classical systems. The list goes on. The question arises to what extent these typically 'quantum' features are entwined and interdependent.

This line of enquiry leads naturally to attempts to construct theories which are 'quantum-like', in that they exhibit *some* typically quantum features, but not others, or they exhibit certain typically quantum features but to a greater or lesser extent than does quantum mechanics itself. Examples of the first type include Spekkens's toy bit theory [32]. Examples of the second type include the 'non-local boxes' [3] which exhibit non-local phenomena to a greater extent than quantum mechanics.

Whilst quantum-like theories, by their nature, make similar predictions, they are expressed in terms of diverse mathematical structures. If they could all be formulated within a single mathematical framework it would facilitate comparison. We could identify precisely in which aspects of this framework different theories differed. We might then hope to identify which mathematical structures within the framework were responsible for which 'typically quantum' features exhibited by different theories. This would help elucidate the inter-relationships between these features: if two 'quantum-like' features corresponded to two independent structures within the framework, we could conclude that the two features were themselves independent. It would also allow for a more systematic cataloguing of quantum-like theories, and facilitate the generation of new ones. It might show that quantum mechanics is not alone in exhibiting all of the 'typically quantum' features, and might point the way to alternative theories which would still account for all of the observed 'quantum' phenomena.

The framework we will use in this work comes out of the work of Abramsky and Coecke [1], in applying category theory to quantum mechanics. A category is an algebraic structure with two kinds of elements, *objects* and *arrows*, or *morphisms*. The structure of a category is

such that, given a physical theory, the systems of a theory are very naturally represented by the objects of a category, and the processes and transformations undergone by the systems are naturally represented by the morphisms. In a category it is the morphisms which have algebraic structure, the objects really just playing the role of labels, and this bias is reflected when we analyse a physical theory in categorical terms. Within this framework we concentrate on the 'algebra of processes' in a theory: how do different physical processes compose together to form new processes? In [1] Abramsky and Coecke originally looked at the category **FHilb**, whose objects and morphisms are the mathematical objects which represent systems and transformations in standard quantum mechanics, and identified the key pieces of structure in this category which facilitated many of the typical features of quantum mechanics. Because of the emphasis on *processes* in the categorical approach, their main concentration, and that of subsequent authors in this field [29, 13, 12, 9] , has been on the information processing tasks made possible by quantum mechanics. However, along with the increased emphasis of how processes combine, there is much less emphasis in this approach on how states and transformations are represented concretely. Thus it seems natural to attempt to use this approach as a unifying framework for different quantum-like theories.

This thesis can be seen as a proof of concept for this programme. Firstly we select an example of a 'quantum-like' theory, Spekkens's toy bit theory [32] and show how it can be re-expressed within the categorical framework. We compare it with quantum mechanics, as expressed with the categorical framework, and show that many of the typically quantum features exhibited by the toy theory correspond to categorical structures which it shares with quantum mechanics. Secondly we analyse a particular example of a typically quantum feature - in this case the impossibility of a local hidden variable interpretation. We identify categorical structures which determine whether or not a given theory has this feature - whether it is 'local' or 'non-local'. Finally we make the link between these two strands and show that the categorical structure where quantum mechanics and Spekkens's toy theory differ is exactly the structure which determines whether or not a theory has an interpretation in terms of local hidden variables. This is exactly what we would expect, since Spekkens's theory is, by construction, a local hidden variable theory.

We now give a more detailed outline of the structure of the thesis.

In **chapter 2**, the first background chapter, we introduce the theories which we will be working with in their standard forms, and discuss some of their key features. We begin, in section 2.1, with a concise account of standard quantum mechanics. The postulates of the theory are introduced, and various characteristic features are discussed, for example, super-positions, incompatible observables, and entanglement. In section 2.2 we give a more detailed account of the key quantum feature with which we will be concerned in this work: the impossibility of replicating the predictions of quantum mechanics with a local hidden variable theory. We go step by step through one of the key 'no-go proofs' which shows that the predictions of quantum mechanics itself cannot be replicated by a local hidden variable theory - this is the argument involving the GHZ state, in the form originally advanced by Mermin [24]. In section 2.3 we introduce a 'sub-theory' of quantum mechanics, *stabiliser quantum mechanics*. This theory involves only one type of system, a *qubit*, and these systems exhibit a restricted class of quantum states, the *stabiliser states* which we define and give several examples of. The stabiliser theory is important in this work, because it is the fragment of quantum mechanics most closely modelled by our key example of a quantum-like theory, Spekkens's toy theory. As

a result it is generally more illuminating to compare the toy theory with the stabiliser theory, rather than with the full quantum theory. Spekkens's toy theory [32] is finally introduced in section 2.4. We begin by introducing the key concepts lying behind the theory, in particular the *knowledge balance principle*, and then use these to derive the form of the states and transformations for some simple systems. We discuss those 'typically quantum' features the theory exhibits, and those which it is unable to replicate. A key sense in which the toy theory is not like quantum mechanics, or stabiliser theory, is that it is, by construction, a local hidden variable theory, and thus it will not be possible to construct 'no-go proofs' of the sort detailed in section 2.2. We conclude our account of the toy theory by asking how well-defined and consistent the theory is, in its original presentation by Spekkens. We conclude that there is some ambiguity in the definition of the theory, and furthermore that the consistency of the states and transformations derived in [32] with the underlying principles of the theory has not been clearly established.

In **chapter 3**, the second background chapter, we introduce the categorical framework within which we intend to compare and contrast quantum-like theories. We begin by giving the basic definitions of categories, functors and natural transformations. We introduce the concept of the *physical category* of a theory - this is the algebraic structure formed by its morphisms, for example, the physical category of quantum mechanics is **FHilb**. The concept of a *symmetric monoidal category* (SMC) is then introduced, and we note that the physical category of *any* physical theory must be symmetric monoidal. A SMC has extra algebraic structure, allowing both objects and morphisms to be combined, and in a physical category this is naturally interpreted as the action of combining systems together to form a larger composite system. In section 3.2 we go on to introduce further categorical structures which we expect the physical category of *quantum-like theories* to possess, since these are the structures which give rise to key quantum-like features in the theory. The main structure in which we are interested is the *basis structure* to which we devote section 3.3. The basis structure is defined abstractly, and we then note that in **FHilb** it corresponds precisely with the notion of an orthonormal basis. Associated with any basis structure is an Abelian group, termed the *phase group*, and we describe the derivation of this group from the basis structure. Lastly we note that from the basis structure we can derive an abstract notion of *GHZ state*. In **FHilb** this notion coincides with the standard GHZ state as introduced in section 2.2. In that section we noted that in standard quantum mechanics the GHZ state is crucially involved in the question of whether or not the theory can be modelled by local hidden variables, and this will turn out to be true in the more general categorical setting as well. Finally in section 3.4 we introduce the category **Stab**. We demonstrate that **Stab** is the physical category of the stabiliser theory, and then go on to investigate the properties of its basis structures. In particular we note that the phase groups of the basis structures of the simplest object are all isomorphic to Z_4. This will be crucial in our later discussion of locality.

In **chapter 4**, the first chapter of original work, we show how to express our key example of a quantum-like theory, Spekkens's toy theory, within the categorical framework. In section 4.1 we define a category **Spek**, a sub-category of **FRel**, the category whose objects are sets and whose morphisms are relations. The definition of **Spek** is constructive: it is defined as the closure under certain operations of a set of generating sets and relations. In the next section, 4.2, we derive the general form of the relations which constitute the morphisms of **Spek**. In fact this derivation is very lengthy, and most of the details are relegated to appendix A.

Section 4.2 does contain a sketch which outlines the essential structure of the proof. In section 4.3 we introduce a second category **MSpek**, derived from **Spek**. Section 4.4 we go on to show that the morphisms of **MSpek** must all be contained in the physical category of the toy theory, and furthermore, allowing for the ambiguity in definition of the toy theory, **MSpek** is a good candidate to act as the physical category of the theory. As a by-product of this analysis we establish that the states and transformations derived by Spekkens in his original paper are indeed consistent with the knowledge balance principle, the key idea underlying the theory. Finally in section 4.5 we investigate the basis structures of **Spek**. We show that they display a very similar structure to those of **Stab**, but crucially, the phase groups of the basis structures of the simplest object in this case are all isomorphic to $Z_2 \times Z_2$. Overall the key results achieved in this section are the following:

- We deduce the physical category for Spekkens's toy theory, thus showing how to incorporate a key example of a quantum-like theory into the categorical framework.
- We demonstrate the consistency of the states and transformations derived in Spekkens's original paper [32] with the key principles underlying that theory.

In **chapter 5**, the second chapter of original work, we develop a categorical treatment of the key feature of quantum-like theories which we hope to investigate - the question of whether or not the predictions of the theory can be reproduced by a local hidden variable theory. To date, the principal application of the categorical approach to quantum mechanics has been the analysis of quantum protocols and information flow in quantum systems. The traditional pre-occupations of quantum physicists - the values of observables, and probabilities of measurement outcomes - have been somewhat neglected. Clearly however, in the analysis of hidden variable interpretations, the issue of the probabilities of measurement outcomes is crucial. In sections 5.1 to 5.4 we develop the ideas necessary for a treatment of this issue. We note that the categorical framework is very well suited for a discussion of *possibilistic* theories - theories which tell us whether an outcome is possible or not, without giving the full quantification of probabilities. The toy theory and stabiliser theory both fit quite naturally into this framework since they allow only a very narrow range of probabilities to be exhibited in measurements. Furthermore, the possibilistic framework is all that is necessary for a treatment of the kind of 'no-go theorem' against hidden variables that we will be subsequently interested in. Nonetheless, we show that the categorical framework is broad enough to accommodate a wider range of notions of probability. In section 5.5 we present an abstract treatment of hidden variables, which applies to any suitable physical category. In sections 5.6 and 5.7 we extend this treatment, to capture the notion of *local* hidden variable theory. Overall the key result of this section is:

- The development of an abstract categorical treatment of local hidden variables, which allows us to discuss this issue in the physical categories of a wide range of theories.

In **chapter 6**, the third chapter of original work, we bring together the work from the previous two chapters. In section 6.1, we note that the categorical structures of **Stab** and **Spek** are very similar, but we pinpoint a key difference: as was noted already, the phase groups of the basis structures on the simplest objects are both four element groups, but in **Stab** the

group is Z_4 and in **Spek** the group is $Z_2 \times Z_2$. The main result of this chapter is that this structural difference between the two physical categories is what underlies a key physical difference between the two theories: the possibility or otherwise of a local hidden variable interpretation. We noted earlier that a phase group is derived from a basis structure, and that it is also possible to derive a generalised GHZ state from a basis structure. Furthermore, we know that in standard QM, GHZ states are an important ingredient of a 'no-go proof' ruling out hidden variables. In sections 6.2 to 6.4, via basis structures, we make the connection between the phase groups and generalised GHZ states of a physical category, and go on to show that if the phase group is Z_4 then the corresponding GHZ state can be used to construct an abstract version of the Mermin no-go argument, whilst if the phase group is $Z_2 \times Z_2$, such an argument is not possible. In the final section we generalise this result to a larger range of phase groups. We show, if a basis structure has one of a certain class of phase groups, it is possible to generalise the structure of the Mermin argument. We then give an entirely group theoretic criterion for which of these groups allow for the crucial contradiction that powers the Mermin argument. Any physical category with a basis structure with such a phase group, must represent a non-local theory.

The main results of this section are the following:

- A demonstration that a key structural difference between the categories **Spek** and **Stab** - differing phase groups - precisely underlies the major physical difference between the two corresponding theories - the possibility of an interpretation in terms of hidden variables.
- A general result classifying a wide range of phase groups into those which facilitate an abstract 'no-go' argument ruling out a hidden variable interpretation and those which do not.

Some of the work appearing has already been published in [10], co-authored with Bob Coecke, and [11], co-authored with Bob Coecke and Rob Spekkens. This is discussed in more detail at the beginning of each chapter.

Chapter 2

Background: quantum theory and quantum-like theories

In this chapter we introduce quantum mechanics and review some of the key features of this theory. We will particularly focus on the feature which will occupy us in the later stages of this work - the possibility or otherwise of hidden variable interpretations of a theory. We will also introduce a restricted version of quantum mechanics, *stabiliser qubit quantum mechanics*, and investigate which of the features of full QM survive the restriction. Finally we will introduce our key example of a *quantum-like* theory, Rob Spekkens's *toy bit theory*.

2.1 Basic quantum mechanics

Quantum mechanics is a framework in which physical theories about microscopic objects can be formulated. In contrast, classical physics is a framework which accommodates theories about systems on a scale which we can observe directly. When physicists attempted to devise theories describing very small systems, like atoms and molecules, they found that these theories could not be accommodated by classical physics. The description of these small systems required concepts quite different to the ones employed in all classical theories. Different microscopic systems behave in wildly different ways and will require different theoretical descriptions, but in all these descriptions the same basic quantum mechanical concepts are employed. We will focus here on the structural features of the quantum framework, leaving aside any details of actual physical systems and their attributes, so our account will seem quite abstract.

2.1.1 The basic postulates of QM

1. The *state* of a system is described by a vector in a Hilbert space $\mathcal{H}$, known as the *state space* of the system.

In fact, multiplying a state vector by any complex number yields a vector describing the same state. So states really correspond to one dimensional subspaces or *rays* of the state space. In fact, we always choose state vectors to be normalised to have a magnitude of 1.

2. The state of a system evolves over time according to: $\psi(t) = U(t, t_0)\psi(t_0)$ where $U(t, t_0)$ is a *unitary* operator on the state space (i.e. $U^{-1} = U^\dagger$), and $\psi(t)$ is the state vector of the system at time t.

The choice of state space and unitary operator depend on the system. Constructing specific theories of quantum systems basically comes down to determining the appropriate state space and unitary evolution operator.

So far the postulates refer only to an abstract state vector and its evolution. They tell us nothing interesting about the properties of the system. The next postulate fills this gap:

3. Associated with each observable property of a system is an Hermitian operator A (an Hermitian operator satisfies $A^\dagger = A$. Such an operator can easily be shown to have real eigenvalues and orthogonal eigenvectors.). If the value of this observable for a system in state ψ is measured:

   (a) The value of the observable will be equal to one of the eigenvalues of the corresponding operator.

   (b) The probability that a particular value a is obtained is given by $|\langle u_a|\psi\rangle|^2$ where u_a is the eigenvector corresponding to the eigenvalue a, and $\langle -|-\rangle$ denotes the inner product defined on $\mathcal{H}$.

   (c) After measuring a value a the state vector of the system instantaneously changes from ψ to u_a. This "leap" into a new state is non-unitary evolution in general. Measurement is the only time when evolution of the state vector is non-unitary.

Two points about this third postulate are immediately surprising. First, QM offers only probabilistic predictions about the values of a system's observables. Second, the appearance of "measurement" in the postulate is surprising. This seems to require an observer or measurer. Can't we just talk about the probabilities that the value of an observable has some value at some time, rather than the probability that a measurement of the observable yields some result? In fact, this is not possible. Observing a quantum system inevitably disturbs it.

4. If one quantum system has state space $\mathcal{H}_1$ and a second system has state space $\mathcal{H}_2$ then if we treat these two systems as one single compound system, its state space is the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$.

The consequences of this postulate are examined further in section 2.1.7.

2.1.2 Dirac notation

Physicists frequently make use of *Dirac* notation, an alternative notation for vectors in a Hilbert space, motivated by the fact that QM frequently employs inner products. A vector in the state space $\mathcal{H}$ is denoted by a *ket* $|\psi\rangle$. A vector from the dual space $H^\star$, consisting of linear maps $\mathcal{H} \to \mathbb{C}$ is denoted by a *bra* $\langle\phi|$. Applying a bra to a ket yields a complex number, equal to the inner product: $\langle\phi|\psi\rangle$; Dirac called this a *bra(c)ket*. If A is an operator on $\mathcal{H}$, then $\langle\phi|A|\psi\rangle$ means $\langle\phi|A\psi\rangle$ in standard notation.

2.1.3 Projection operators

A *projection operator* or *projector* P is a linear operator on $\mathcal{H}$ which is both Hermitian and idempotent (i.e. $P^2 = P$). It can be shown that these properties imply that a projector will project vectors onto a certain subspace, and that the subspaces and projectors of $\mathcal{H}$ are in bijective correspondence. It can further be shown that any Hermitian operator A can be written as $A = \sum_i a_i P_i$ where the a_i are real and the P_i are projectors satisfying $P_i P_j = \delta_{ij} P_i$ and $\sum_i P_i = 1$. This is known as the *spectral decomposition* of A. In fact the a_i are the eigenvectors of A and the P_i project onto the subspaces spanned by the eigenvectors with eigenvalue a_i.

The way we phrased the third postulate of QM actually relied on that fact that the observable A had no degenerate eigenvectors i.e. eigenvectors with the same eigenvalue. We can reformulate the third postulate to cope with degeneracy using projectors:

3(b)′. The probability of obtaining measurement outcome a_i when the system is in state $|\psi\rangle$ is given by $\langle\psi|P_i|\psi\rangle$.

3(c)′. Immediately after measurement the system's state vector becomes $\frac{P_i|\psi\rangle}{||P_i|\psi\rangle||}$.

In the case of no degeneracy these can easily be shown to reduce to the postulates as originally stated (noting that the projector onto a one-dimensional subspace can be written as $|\psi\rangle\langle\psi|$ where $|\psi\rangle$ is a normalised vector within the subspace) .

2.1.4 Superposition

The eigenvectors of an observable A are orthogonal, can be normalised, and furthermore they span the whole space $\mathcal{H}$. This means that any state vector $|\psi\rangle$ can be written in terms of the eigenvectors of A, which we will write as $|a_i\rangle$:

$$|\psi\rangle = \sum_i \psi_i |a_i\rangle \tag{2.1}$$

where the ψ_i are complex numbers. Note that:

$$\langle a_j|\psi\rangle = \sum_i \psi_i \langle a_j|a_i\rangle = \sum_i \psi_i \delta_{ij} = \psi_j \tag{2.2}$$

Thus, referring to postulate 3b we see that the probability of measuring A to have a value a_i is given by $|\psi_i|^2$. The only states for which we will get a definite, predictable outcome for a measurement of A are the eigenstates $|a_i\rangle$ of A. It is only for these states that A has a definite value. Any other states are referred to as *superpositions* of A eigenstates; these states do not have definite values for A.

2.1.5 Incompatible observables and mutually unbiased observables

In general, the Hermitian operators associated with two different observables A and B will not have the same eigenvectors.

Proposition 2.1.1 Two operators A and B will share the same eigenvectors *iff* $AB = BA$, i.e. if they *commute*. Such a pair of observables is termed *compatible*, all other pairs of observables being *incompatible*.

The eigenvectors of incompatible operators A and B both constitute bases in which a general vector can be expanded:

$$|\psi\rangle = \sum_i \psi_i^A |a_i\rangle = \sum_i \psi_i^B |b_i\rangle \tag{2.3}$$

The different coefficients ψ_i^A and ψ_i^B can be squared to give the different probability distributions for the outcomes of measurements of A and B.

Note that an eigenstate of A, $|a_i\rangle$ will be expandable in terms of more than one eigenvector of B:

$$|a_i\rangle = \sum_j \alpha_j |b_j\rangle \tag{2.4}$$

Thus for incompatible A and B, a state with a definite value of A will *not* have a definite value for B, and vice versa.

It's possible to identify pairs of observables which are, in some sense, maximally incompatible.

Definition 2.1.2 A vector $|\psi\rangle$ is *unbiased* with respect to a basis $\{|a_i\rangle\}_{i=1\ldots n}$ if for all i:

$$\langle a_i|\psi\rangle = \frac{1}{\sqrt{n}} e^{i\phi} \tag{2.5}$$

where $0 \leq \phi < 2\pi$.

Definition 2.1.3 Two observables A and B, on an n-dimensional Hilbert space, are *mutually unbiased* if the eigenstates $|a_i\rangle$ of A are all unbiased with respect to the eigenstates $|b_j\rangle$ of B, and vice versa.

The interpretation of this result is that if the system is in an eigenstate of A, then a measurement of B has an equal chance of yielding any of the possible outcomes of B, and vice versa. If we have full knowledge of the value of one of the observables, we know nothing about the value of the other.

2.1.6 Qubits and Pauli operators

The simplest non-trivial example of a quantum system is one described by a two-dimensional state space. Such a system is termed a *qubit*. There are many physical realisation of qubits, for example the spin state of an electron, the polarization state of a photon, but as we mentioned at the beginning of this section we are interested in the structural properties of states and transformations shared by all qubits, rather than the details of any particular realisation.

We will be focussing heavily on qubits throughout this work for several reasons. As the dimension of a state space grows, the number and complexity of states and transformations also grows very quickly. Qubit systems are simpler to deal with than larger dimensional systems, yet still exhibit all of the 'typically quantum' phenomena we are interested in (it is true that in some senses the 2-dimensional case is somewhat 'degenerate' leading to some phenomena specific to it, but these will not concern us in this work).

When dealing with qubits there are three observables in which we are particularly interested. These are represented by three Hermitian operators X, Y and Z which are known as the *Pauli operators*. The properties of these operators are neatly summarised by this relation:

$$X^2 = Y^2 = Z^2 = I \tag{2.6}$$

where I is the identity operator, and this one:

$$XY = iZ, \quad YX = -iZ \tag{2.7}$$

along with all its cyclic permutations. From these simple relationships one can derive all of the properties of these operators (see for example [28]). The first relation for example implies that the eigenvalues of these operators are ± 1.

The eigenstates of the Z operator are conventionally denoted as $|0\rangle$ and $|1\rangle$. It is also conventional to use these vectors as the 'default' basis for the state space of a qubit. Due to the importance of qubits in the field of quantum computation and information this is often referred to as the *computational basis*. Expressed in the computational basis, the matrix representations of the Pauli operators are:

$$X : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y : \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z : \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.8}$$

The eigenstates of X are conventionally denoted $|+\rangle$ and $|-\rangle$, and in the computational basis are written:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.9}$$

whilst the eigenstates of Y are conventionally denoted $|i\rangle$ and $|-i\rangle$, and in the computational basis are written:

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \tag{2.10}$$

Comparison with equation 2.5 indicates that X and Z, and Y and Z are mutually unbiased pairs of observables, and a straightforward calculation shows that X and Y also are.

Consider the 16 element set consisting of X, Y, Z and I, along with multiples of these operators by the scalar factors -1, i and $-i$. It is straightforward to verify, using relations

2.6 and 2.7 that this set is closed under composition of operators, and furthermore satisfies all of the axioms of a group. This group is termed the *Pauli group on 1 qubit*. The *Pauli group on n qubits* consists of all n-fold tensor products of the three Pauli operators and the identity, and the -1, i and $-i$ multiples of these. For example, $X \otimes X$ and $i(Y \otimes Z)$ are elements of the Pauli group on two qubits. Note that the elements of the Pauli group with scalar factors of 1 and -1 are Hermitian, whilst those with scalar factors of i and $-i$ are *anti-Hermitian* (i.e. $A^\dagger = -A$).

2.1.7 Compound systems, separable and entangled states

Our fourth postulate in section 2.1.1 noted that the compound system of two systems with state spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ has as its state space the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$.

For any pair of vectors $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$ we have a *product* vector or *separable* vector in the tensor product space denoted by $|\psi\rangle \otimes |\phi\rangle$. Most vectors in $\mathcal{H}_1 \otimes \mathcal{H}_2$ however, are linear superpositions of such product vectors, and cannot be written as a product vector themselves. To see this, assume that $\{|i\rangle\}_{i=0,m-1}$ and $\{|j\rangle\}_{i=0,n-1}$ constitute orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, so that we can write $|\psi\rangle \otimes |\phi\rangle$ as:

$$|\psi\rangle \otimes |\phi\rangle = \sum_{i,j} \psi_i \phi_j |i\rangle \otimes |j\rangle \tag{2.11}$$

Now by the definition of the tensor product it's clear that the vectors $\{|i\rangle \otimes |j\rangle\}$ form a basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$. Thus we can write a general vector $|\Psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ as:

$$|\Psi\rangle = \sum_{i,j} \Psi_{i,j} |i\rangle \otimes |j\rangle \tag{2.12}$$

Clearly, the majority of the choices for the numbers $\Psi_{i,j}$ will not be decomposable as $\psi_i \phi_j$.

Definition 2.1.4 A quantum state vector in a tensor product state space which is *not* a product vector is called an *entangled* state.

A well-known example of such as state, in the case that the two spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ have the same dimension, is the *Bell state*:

$$|\Psi_{\text{Bell}}\rangle = \frac{1}{\sqrt{m}} \sum_i |i\rangle \otimes |i\rangle \tag{2.13}$$

In a classical theory to specify the state of a compound system we merely need to specify the states of all of its components. Entanglement means that the situation is different in QM. Even if the entangled systems are separated by great distances we must in some sense view them as a single system.

Given linear operators $f_1 : \mathcal{H}_1 \to \mathcal{H}_1$ and $f_2 : \mathcal{H}_2 \to \mathcal{H}_2$ we can form an operator $f_1 \otimes f_2$ acting on the tensor product space. Such an operator is interpreted as performing separate operations on the two component parts of the system. It is straightforward to show that such a *local* operator *cannot* map a product state into an entangled state although the reverse

is possible. This leads to a notion of ranking the entanglement in different states. Very loosely, a state $|\Psi\rangle$ is deemed to have greater or equal entanglement to a state $|\Phi\rangle$ if it is possible to map $|\Psi\rangle$ to $|\Phi\rangle$ via local operations. For compound systems with just two components (*bipartite systems*), it is possible to rank all states like this into a well-defined hierarchy (actually a pre-order) [25]. At the top of this order are the Bell state and all states which can be reached from it by applying *local unitary* operations (local operations in which all of the constituent maps are unitary). These Bell-type states are thus deemed to be the *maximally entangled* bipartite states. For compound systems with more than two components (*multipartite systems*) the situation is much more complicated, and determining this hierarchy of states under local operations is still an unsolved problem, though there do exist some coarser-grained classifications of multipartite entanglement [15].

One can map a product state into an entangled state by using an operation which is not local. This corresponds to an operation in which the subsystems interact directly. As an example consider the case of a pair of qubits, and the following operation, termed the *controlled-NOT gate* or CNOT gate:

$$U_{\text{CNOT}} :: \begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |10\rangle \to |10\rangle \end{cases} \tag{2.14}$$

so called because, in the computational basis, the first qubit acts as a control: if it is 0 the identity is applied to the second qubit, if it is 1 the value of the second qubit is flipped. Observe the effect of the CNOT gate on the separable state $|+\rangle \otimes |0\rangle$:

$$U_{\text{CNOT}}(|+\rangle \otimes |0\rangle) = U_{\text{CNOT}}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.15}$$

2.1.8 Quantum teleportation

The structure of quantum mechanics allows for many information processing tasks to be performed which would not otherwise be possible at all, or would only be possible with much lower efficiency. Information is encoded in the states of quantum system and is then processed through the appropriate application of unitary operators, or measurements. Examples include quantum computing algorithms for factoring numbers [30], quantum cryptography protocols [5] for secure communication, and a host of other protocols. We present one particular protocol here, quantum teleportation [6], both because it provides a good example of quantum information processing, and because it is a feature which is replicated in the quantum-like theories we will later be considering.

The protocol involves two parties traditionally known as Alice and Bob. Alice begins with a single qubit in an unknown state:

$$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle \tag{2.16}$$

Alice and Bob also have one qubit each of an entangled two-qubit system. These two qubits are collectively described by the qubit Bell state:

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{2.17}$$

The aim of the protocol is for Alice to transmit the information about the state of her qubit to Bob, so that he is able to prepare a qubit in the same state, *without* Alice actually sending her qubit to Bob. Alice and Bob can exchange classical information, but they cannot send any qubits between one another. Naively one might think that Alice could simply determine her state and send the information about that state (i.e. the complex numbers ψ_0 and ψ_1 from equation 2.16) to Bob over the classical channel. But given a single copy of $|\psi\rangle$ how would Alice determine these coefficients? If she performs any measurement on the state she will get one outcome or the other with a certain probability. Attempting to measure the system will collapse the state vector into one or other eigenvector.

In fact Alice and Bob proceed as follows. The state of the three qubits is initially $|\psi\rangle \otimes |\Psi^+\rangle$. Alice performs a measurement on the two qubits she possesses (one that she's aiming to teleport, and one half of the Bell pair) in the Bell basis. The Bell basis is spanned by:

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{2.18}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \tag{2.19}$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) \tag{2.20}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \tag{2.21}$$

What happens to the state of the three qubits depends on the measurement outcome. If, for example, the fourth measurement outcome is realised, the new state of the three qubits is given by:

$$(|\Phi^-\rangle\langle\Phi^-| \otimes 1)(|\psi\rangle \otimes |\Psi^+\rangle \tag{2.22}$$

and similarly for the other measurement outcomes. The next step in the protocol is for Alice to communicate the result of the measurement over the classical channel to Bob. Since there are four possible outcomes, Alice needs to send only two classical bits of information over the channel. Depending on the information which he receives from Alice, Bob then performs one of four unitary correction operations on his qubit (which was originally one half of the Bell pair). The remarkable result of the protocol, proved in the original paper [6], is that after making the appropriate correction Bob's qubit will be in the state $|\psi\rangle$.

A particularly remarkable aspect of this protocol is this: according to equation 2.16 it takes two complex parameters to describe the state $|\psi\rangle$. In fact the state will be normalised and the overall phase of the state is physically unimportant. Nevertheless this leaves two continuous real parameters needed to completely specify $|\psi\rangle$. But Alice sends just two bits of information over the classical channel to Bob, and from this he is able to reconstruct $|\psi\rangle$. Somehow the entangled state shared by Alice and Bob must act as a kind of channel to transmit the rest of the information.

2.1.9 Mixed states, POVMs, completely positive maps

The description of the axioms of quantum mechanics in section 2.1.1 assumes a closed quantum system. It also assumes that we have the maximum possible knowledge about the system. If either of these conditions doesn't hold, in the case of an open system, or incomplete knowledge, an alternative set of mathematical structures are employed to describe quantum systems (see for example [26]).

- A system is still associated with a Hilbert space $\mathcal{H}$.
- The state of a system is described by a *density operator* $\rho : \mathcal{H} \to \mathcal{H}$, a positive Hermitian operator with trace equal to 1. Such a state is termed a *mixed state*. In contrast we refer to the states described by state vectors, which were introduced in section 2.1.1, as *pure states*.
- Measurements are described by *positive operator value measurements* or POVMs.
- The evolution of the system is described by a *completely positive map*, a map of type $(\mathcal{H} \to \mathcal{H}) \to (\mathcal{H} \to \mathcal{H})$ which preserves the defining properties of a density operator.

We will make very little use of these concepts in what follows, since they complicate matters, and the phenomenon in which we are primarily interested, the issue of hidden variables, can just as easily be exhibited in the pure state formalism.

2.2 Hidden variable theories and no-go theorems

2.2.1 Hidden variable interpretations

In QM the most complete description of a system is given by a pure state vector $|\psi\rangle$. Given this vector, for any observable A of the system, we can derive a probability distribution $p(A = a) = |\langle a|\psi\rangle|^2$. This tells us the probability of obtaining each possible outcome a, if we measure observable A. Probably the most natural conclusion to draw is that QM is not a complete description of nature, but is some kind of 'statistical' theory, reflecting a lack of knowledge of the exact state of the system. The following statements would be typical of such a view:

- The systems described by quantum mechanics possess well-defined definite values for all their observable quantities. Specifying all these values would give us the true state of the system. We will refer to this as the 'ontic' state of the system - it would tell us how the system actually *is*.
- However, in practice, we never have a situation where we know the ontic state exactly. Instead the best state of knowledge we can have is a probability distribution over the ontic states. This restriction on our knowledge might be practical, simply a deficiency of our technical abilities in probing and manipulating quantum systems, or it might have some more fundamental origin. Each quantum state would correspond to a particular probability distribution over the ontic states, and conversely, these are the only distributions allowed. We would denote such a distribution by:

$$p_\psi(A = a, B = b, C = c \dots) \tag{2.23}$$

where ψ is the QM state, $A, B, C \dots$ are the observables for the system, and $a, b, c \dots$ range over the possible values the observables can take.

- The probabilities which we obtain from the quantum state via the Born rule are equal to the marginal probabilities obtained from the distribution over ontic states. For example, if $A, B, C \ldots$ are the observables of the system, the probability distribution over values for A would be given by these equivalent formulae:

$$|\langle a|\psi\rangle|^2 = \sum_{b,c\ldots} p_\psi(A = a, B = b, C = c \ldots) \tag{2.24}$$

  the LHS being the value derived from the QM state vector, and the RHS coming from the probability distribution over the ontic states.

These statements seem so obviously and necessarily true that one may wonder why we are bothering to spell them out. The reason is that, unless combined with some other rather bizarre assumptions, they are actually incompatible with the predictions of quantum mechanics. We will shortly examine some of the ways in which this can be shown, but we will pause briefly here to consider what this means for the ontology of a world described by QM.

An attempt to interpret QM according to the statements above is traditionally termed a *hidden variable* interpretation (HVI). The origin of this terminology is the idea if we wanted to know the exact 'ontic' state of a system we need to know both the QM state vector, and the value of additional variables, which in practice are 'hidden' from us. Although the literature can sometimes be confusing on this issue, without loss of generality we can take these hidden variables to be the values of the observables themselves. Perhaps the key point about this type of interpretation is the idea that systems possess well-defined values for the observables at all times, regardless of whether any observer is measuring them, and for this reason a better term might be '*realist* interpretation'. A theory which can be given a hidden variable interpretation is termed a *hidden variable theory* or HVT.

Almost from the beginning of QM claims were made to have shown that there could be no HVI for QM [34]. However the majority view is that these early arguments were all flawed and it was not until the 1960s that two convincing 'no-go' arguments were put forward, ruling out HVIs for QM. These were *Bell's theorem* [4], and the *Kochen-Specker theorem* [22]. These arguments were extremely significant in the history of the understanding of the hidden variable issue, but they have to some extent been superseded by subsequent simpler or more elegant arguments, one of which we now present in detail.

2.2.2 The GHZ no-go argument

By far the simplest and most convincing no-go argument was proposed in 1989 [18] and reworked into the form which we will discuss here in 1990 [24]. This argument employs three qubits in the following quantum pure state:

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{2.25}$$

where $|0\rangle$ and $|1\rangle$ are the eigenstates of the Pauli Z operator. This state is known as the Greenberger-Horne-Zeilinger state or GHZ state, after the authors of the 1989 paper.

What are the predictions of a realist/hidden variable interpretation of this state? Any three qubits in this state will each possess a well-defined, at-all-times-existing value for each of its observables. For reasons which will become apparent below, we are particularly interested in the Pauli X and Y observables. These can each take two values, +1 and -1. There are $2^6 = 64$ possible combinations of values which they can take for the three qubits. Any given system of three qubits should have one of these combinations of values.

What are the predictions of QM? It is straightforward to verify that this state is an eigenstate of the observable $(X_1 \otimes X_2 \otimes X_3)$ with eigenvalue +1. This implies that if we measure the X observable on each qubit our triple of outcomes must multiply together to give +1. Put another way, the triple of outcomes must have +1 occurring an odd number of times. Put yet another way the outcome triples (1,1,1), (1,-1,-1), (-1,1,-1) and (-1,-1,1) may all occur while the other four will never occur. Simultaneously the GHZ state is an eigenstate of the observables $(X_1 \otimes Y_2 \otimes Y_3)$, $(Y_1 \otimes X_2 \otimes Y_3)$ and $(Y_1 \otimes Y_2 \otimes X_3)$, in each case with eigenvector -1. In these cases, in contrast to the $(X_1 \otimes X_2 \otimes X_3)$ case, the triple of outcomes must have +1 occurring an even number of times.

Are the predictions of the HVI and QM compatible? It turns out that they are not. This failure of compatibility is quite extreme – none of the 64 possible assignments of values to the six observables (X_1, X_2, X_3, Y_1, Y_2, and Y_3) satisfies the parity conditions described in the paragraph above. We could verify this by going through each of the 64 assignments, one by one, and checking whether they satisfy the parity conditions, but there is a more elegant and much easier way to show it.

We begin by constructing what we will refer to as a *Mermin* table. We take the four observable triples and arrange them in four rows. We then have a four-by-three array of observables, with each observable appearing twice:

$$\begin{array}{ccc} X_1 & X_2 & X_3 \\ X_1 & Y_2 & Y_3 \\ Y_1 & X_2 & Y_3 \\ Y_1 & Y_2 & X_3 \end{array}$$

Suppose we pick a particular one of the 64 possible assignments, and input the values into this table. Multiply all the values together. Do we get +1 or -1?

We can work this out in two ways. The first way is to figure out the result of multiplying the entries of each row, and then multiplying these three numbers together. The result for each row is already given to us by the QM predictions: for the first row it is +1, and for the other rows it is -1. Thus the product of all the entries in the table should be -1.

$$\begin{array}{ccccc} X_1 & X_2 & X_3 & & +1 \\ X_1 & Y_2 & Y_3 & & -1 \\ Y_1 & X_2 & Y_3 & & -1 \\ Y_1 & Y_2 & X_3 & & -1 \\ & & & & = -1 \end{array}$$

The second way is to figure out the result of multiplying the entries of each column, and then multiplying these three numbers together. Each column has four entries - two observables each

appearing twice. Presumably each appearance of the same observable in the table should be assigned the same value (a key assumption which will be re-examined below), so multiplying these two identical values together should yield +1, making each column product +1. This implies that the product of all entries in the table should be +1, and we have a contradiction with the first calculation.

$$\begin{array}{cccc} X_1 & X_2 & X_3 & \\ X_1 & Y_2 & Y_3 & \\ Y_1 & X_2 & Y_3 & \\ Y_1 & Y_2 & X_3 & \\ +1 & +1 & +1 & = +1 \end{array}$$

We conclude that there is no way of assigning well-defined values to the six observables which is consistent with the predictions of QM.

This result is problematic for the proponent of hidden variables. According to the HVI the system of three qubits must have definite values for X and Y for each qubit. We can choose to measure any triple of observables, and this measurement will reveal the pre-existing definite value of those observables. In particular we could choose to measure $(X_1 \otimes X_2 \otimes X_3)$, $(X_1 \otimes Y_2 \otimes Y_3)$, $(Y_1 \otimes X_2 \otimes Y_3)$ or $(Y_1 \otimes Y_2 \otimes X_3)$. The QM predictions claim that the outcomes of these measurements must obey certain parity conditions. But there is no way that we could assign values to each of the six observables in such a way that we could choose to measure any one of the four observable triples, and still get results which respected the parity conditions.

2.2.3 Non-local hidden variables

There is an escape from the GHZ argument for the hidden variables proponent. In the argument using the Mermin table, a key assumption was that both appearances of each observable in the table should be assigned the same value. If this requirement was not in place, there would be no constraints on the column products, and would be able to fill in the table, happily obeying the constraints on the row products.

This is all very well as a mathematical manoeuvre, but what does it mean physically? To answer this we need to ask: why did we initially require each instance of a given observable in the table to take the same value? For example, consider the appearances made by X_1 in the first and second rows of the table.

$$\begin{array}{ccc} \underline{X_1} & X_2 & X_3 \\ \underline{X_1} & Y_2 & Y_3 \\ Y_1 & X_2 & Y_3 \\ Y_1 & Y_2 & X_3 \end{array}$$

It seems to make sense that these should both take the same value - in a realist interpretation a physical quantity has one definite value. However, suppose we allow for the possibility that the choice of which measurements to make on the second and third systems, either X on both, or Y on both, is in some way capable of disturbing the value of X possessed by the first system. Then the two appearances of X_1 in the table need not necessarily be assigned the same value.

This disturbance would need to be instantaneous, because the quantum predictions hold, regardless of what distances separate the particles, and what intervals separate the measurements.

Thus, the predictions of quantum mechanics are compatible with the idea of systems possessing well-defined values for their observables, so long as we allow that these values can be instantaneously disturbed by actions performed on other systems, potentially separated from the initial system by great distances. Indeed there do exist famous examples of realist interpretations of quantum mechanics, which have exactly this non-local character [8]. Not surprisingly, such a theory is termed a *non-local hidden variable theory*. Strictly then, the GHZ argument only rules out a *local hidden variable* interpretation of quantum mechanics.

2.3 Stabiliser quantum mechanics

We now consider a 'sub-theory' of standard quantum mechanics, in which the only systems are qubits, and which involves only a subset of the states and operations of QM. The states concerned are termed the *stabiliser states*, which give their name to the theory.

2.3.1 Stabiliser states

We say that a state $|\psi\rangle$ is *stabilised* by a linear operator A if it is an eigenstate of that operator with eigenvalue $+1$, i.e. $A|\psi\rangle = |\psi\rangle$. If all vectors in a subspace are stabilised by A, then that subspace is said to be stabilised by A.

Recall the definition of the Pauli group on n qubits in section 2.1.6. Consider a commutative sub-group of the Pauli group on n qubits generated by k independent Hermitian operators (a set of Pauli operators are said to be *independent* if none can be obtained as products of the others). It's possible to show (e.g. [16, page 20]), that the members of such a sub-group will simultaneously stabilise a sub-space of dimension 2^{n-k}.

Definition 2.3.1 A *stabiliser sub-group* is a commutative sub-group of the Pauli group on n qubits, generated by n independent Hermitian operators.

Definition 2.3.2 A *stabiliser state* on n qubits is an element of the 1-dimensional subspace stabilised by a stabiliser sub-group.

Stabiliser states form a key ingredient of the *stabiliser formalism* which has important applications in many branches of quantum information theory, and we have included their full definition for completeness. However the details of the definition of a stabiliser state concerns *us* much less than the fact that these states form a discrete subset of the full set of quantum states, which is much easier to work with, but still exhibits many of the key 'typically quantum' features. Here is a brief summary of the stabiliser states for low numbers of qubits:

1. A single qubit has six stabiliser states: $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle$ and $|-i\rangle$, being the $+1$ eigenstates of the following six states $X, -X, Y, -Y, Z$ and $-Z$.

2. There are 60 stabiliser states on two qubits: 36 of these are the product states of the six single qubit states, for example $|01\rangle$, and the other 24 are maximally entangled states, all LU equivalent to the qubit Bell state, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

3. From the discussion in section 2.2.2 the three-qubit stabiliser states clearly include the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Three independent generators for the sub-group which stabilises it are $-X \otimes Y \otimes Y$, $-Y \otimes X \otimes Y$ and $-Y \otimes Y \otimes X$.

2.3.2 Clifford operations and Pauli measurements

Definition 2.3.3 The n-qubit *Clifford unitaries* are those n-qubit unitary operations which map the stabiliser states back into stabiliser states.

It is clear that these operations will form a sub-group of the unitary group $U(n)$, termed the *Clifford group*. It can be shown [19] that, up to a phase factor, there are 24 single-qubit Clifford unitaries, and they form the permutation group S_4.

Proposition 2.3.4 Any n-qubit Clifford unitary can be decomposed into a sequence of single-qubit Clifford unitaries and two-qubit CNOT operations.

Proof: See for example [19]. □

The Clifford unitaries are the unitary operations which preserve stabiliser states. What sort of measurements can be performed which will guarantee that the resulting state is a stabiliser state? If we restrict ourselves to measurement of the observables corresponding to the *Hermitian* elements of the Pauli group, we will ensure that the state of a system, post-measurement, will be one of the eigenstates of these operators, which is bound to be a stabiliser state. Interestingly it can be shown [16, pages 37-8] that any pair of observables from the Pauli group will either commute, or be mutually unbiased. Thus Pauli measurements on stabiliser states will either yield one outcome with certainty, or all possible outcomes with equal probability.

2.3.3 Stabiliser quantum mechanics

In standard quantum mechanics, systems are associated with Hilbert spaces, their states are described by normalised vectors within those spaces, the evolution of these states is described by unitary operators, and observables are described by Hermitian operators, with measurement of these observables occurring as described in the third postulate in section 2.1.1.

Definition 2.3.5 *Stabiliser quantum mechanics* is a sub-theory of standard QM, in which:

- The **systems** are qubits, or collections of qubits.
- The **states** which these systems can occupy are the stabiliser states.

- The **evolution** of the state of a system is described by the Clifford unitaries.

- The **observables** of an n-qubit system are described by the Hermitian elements of the Pauli group on n-qubits. Apart from the restriction on the operators which represent observables, the description of measurement exactly parallels that in standard QM.

This is clearly a well-defined theory, since both evolution and measurement disturbance transform one stabiliser state into another. It is a much simpler theory than QM, having only one type of system, and a discrete set of states and transformations, rather than a continuum. For example, a single system has only three observables, all of which are mutually unbiased. Each of these has two eigenstates, and these six states are the only states which a single system can occupy. Despite this simplicity, stabiliser quantum mechanics still exhibits many of the features which are generally considered typical of quantum mechanics.

- The stabiliser theory has **incompatible observables**, and thus the state of a system cannot simultaneously specify well-defined values for all of its observables. The most obvious examples are the three observables X, Y and Z on the single system. Given a system in state $|+\rangle$ a measurement of X is bound to yield an outcome of $+1$, but measurements of Y or Z could yield either outcome, each with a probability of $1/2$.

- The stabiliser theory exhibits **entanglement**. The entanglement structure is rather simpler than in the case of full QM: for example for a two qubit system states are either separable or maximally entangled - there is no complex hierarchy of bipartite entanglement as described in section 2.1.7. Much of the complexity of multipartite is also missing - for example the W-class states of [15] are not stabiliser states. None the less, considerable complexity remains - the *graph states*, a sub-class of entangled states which have been heavily studied [19] are all stabiliser states.

- All of the essential ingredients of the **teleportation protocol** survive, as do many other **quantum information protocols**, for example dense coding.

- All of the ingredients of the **no-go proof against local hidden variables** described in section 2.2.2, the GHZ state, and measurements of the observables X and Y, survive in stabiliser theory. Thus stabiliser theory has no interpretation in terms of local hidden variables.

2.4 Spekkens's toy bit theory

We now consider our key example of a 'quantum-like' theory, the toy bit theory proposed by Rob Spekkens [32]. Spekkens developed this theory with the aim of demonstrating that many (though not all) of the typically 'quantum' features of QM, can in fact be exhibited by a typically classical system, so long as there is some restriction on our knowledge of the system.

2.4.1 Systems and knowledge balance principle

The theory is very abstract in character - there are 'systems' which can occupy 'states', 'measurements' can be made, but there is no mention of any concrete attributes which a system could possess, such as position, momentum, spin etc. There is only one kind of system in the theory, which is intended to resemble a qubit. We will describe this as the *elementary system*. This system can exist in one of four different states. Spekkens uses the term *ontic state* to describe these states, since they are intended to represent the objectively-existing state of affairs with respect to the system. We will refer to the ontic states of an elementary system simply as 1, 2, 3, and 4; thus the ontic state space is the set $\mathrm{IV} := \{1, 2, 3, 4\}$. The ontic state of a compound system is given by stating the ontic state of each of the elementary constituents, thus the ontic state space for a compound system with n elementary constituents is IV^n - this is in clear contrast to the QM situation.

So far this is simply a very abstract presentation of an essentially classical theory. The key novel feature of Spekkens's theory is that there is a restriction on how accurately we can know the ontic state of a system.

Definition 2.4.1 A *canonical question set* is a set of yes-no questions about the ontic state of a system, which has the minimum number of elements such that the answers uniquely identify the ontic state.

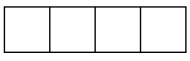
For an elementary system an example of a canonical question set would be the two questions: "Is the ontic state in the set $\{1, 2\}$ or not?", and "Is the ontic state in the set $\{2, 3\}$ or not?". In Spekkens's scheme the only kind of knowledge one can have about the ontic state of a system is to know the answers to some subset of the questions in a canonical set. The 'amount of knowledge' we have is exactly equal to the number of questions we know the answer to. With this concept in mind we are able to state the *knowledge balance principle*:

"If one has maximal knowledge, then for every system, at every time, the amount of knowledge one possesses about the ontic state of the system at that time must equal the amount of knowledge one lacks."

2.4.2 Epistemic states for a single system

We can apply this principle to the elementary system. A canonical question set for an elementary system consists of two questions, and from the knowledge balance principle we deduce that we can know the answer to at most one of these. Thus, in a state of maximal knowledge we know that the system occupies one of two ontic states. Spekkens refers to the state of our knowledge about the system as the *epistemic state*, and it is this which is intended to be the analogue of the quantum state.

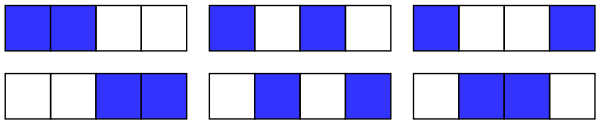
We can represent the ontic state space of an elementary system by:



(2.26)

We then represent an epistemic state by shading those ontic states which the system might occupy when that epistemic state represents the state of our knowledge about the system. Us-

ing this diagrammatic notation, we can depict the six epistemic states of maximal knowledge for an elementary system as:



(2.27)

Note, firstly, that epistemic states are simply subsets of the ontic state space. Any two states which, when viewed as subsets, have an empty intersection, are termed *disjoint*. Disjoint epistemic states are the analogue of orthogonal quantum states. Note, secondly, that these six states fall naturally into three families of two states, where the states of a family are disjoint, and their union is equal to the whole ontic state space. Such a family is the analogue of an orthogonal basis in QM.

There are also epistemic states representing less than maximal knowledge about the system. Non-maximal knowledge, in this context, means knowing the answer to less than half the questions in a canonical set. In the case of an elementary system this implies knowing the answer to no questions. Thus we have just one non-maximal epistemic state:

(2.28)

Such states play an analogous role in the toy theory to mixed states in quantum mechanics.

Spekkens goes on to employ the knowledge balance principle on multiple occasions to derive the allowed states and transformations in his theory. We will come back to this point later on, when we discuss the issue of how well-defined the theory is, but for now we will largely restrict ourselves to simply describing the states, transformations and phenomena of the theory.

2.4.3 Transformations and measurements on a single system

We next consider dynamics: how does the ontic state of a system evolve? Spekkens approaches this question by asking: what transformations on the ontic states lead to transformations on the epistemic states which are allowed by the knowledge balance principle? A transformation on the ontic states of an elementary system is a function of type $\text{IV} \to \text{IV}$. We note that this function must be injective. Imagine that we have a non-injective function, which, for example maps 1 and 2 into the same ontic state. The epistemic state $\{1, 2\}$ would then be mapped into a singleton subset, which is not a valid epistemic state according to the knowledge balance principle. Thus we conclude that the allowed transformations are the *permutations* of the four ontic states. There are 24 such permutations, forming a group, S_4 under composition.

Measurement in the toy theory corresponds to asking as many questions from a canonical set as the knowledge balance principle will allow you answers to. In the case of an elementary system this means asking one question. In fact there are three questions about the ontic state of an elementary system which can form part of a canonical set (any given canonical set contains two of these questions), and thus there are three possible measurements we can perform. Pictorially we denote them as:

A	A	B	B

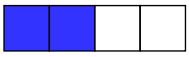
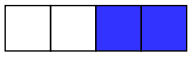
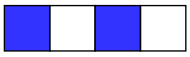
A	B	A	B

A	B	B	A

(2.29)

where the 'A' and 'B' denote the different possible outcomes for the measurement: for example the first measurement amounts to the question: "Is the ontic state one of $\{1, 2\}$ (outcome A) or is it one of $\{3, 4\}$ (outcome B)?".

Suppose we perform the first measurement on elementary systems described by the following three epistemic states:

(i)  (ii)  (iii)  (2.30)

If our system is described by (i), we are certain to get outcome A, because we know that the state has ontic state 1 or 2. If our system is described by (ii) we are certain to get outcome B. If our system is described by (iii) we know that our system is either in ontic state 1 or 3, so we may get either outcome A or outcome B. Spekkens actually goes further and suggests that we will get each outcome with a probability of 1/2, but we can equally well view the theory as giving us certainties, possibilities and impossibilities, rather than probabilities.

The knowledge balance principle implies that any measurement inevitably induces a disturbance on the ontic state. To see this imagine that initially our epistemic state for the system is (iii), and we get outcome A when performing the first measurement. We can now infer that the system was in ontic state 1. However, the knowledge balance principle prohibits us from knowing which ontic state the system is in at the present time. Thus, even though we can infer what the ontic state *was* prior to measurement, there must have been some kind of disturbance of the ontic state during the measurement, so that we can no longer be sure what it *is*. Spekkens also requires that repeated measurements of the same type should yield the same outcome. From these requirements we conclude that the disturbance should be probabilistic, and of the following form. All ontic states consistent with a given outcome of the measurement should be permuted amongst themselves. The different possible permutations should be realised with equal probability. Thus, the first measurement in diagram 2.29 should induce, with equal probability, one of the following four permutations of the ontic states: (1)(2)(3)(4) (i.e. the identity), (12)(3)(4), (1)(2)(34), or (12)(34).

The result of such a disturbance is that if we obtain outcome A the new epistemic state is the one on the left below, while if we obtain B, the new epistemic state is the one on the right:

 (2.31)

If we are considering only epistemic states, the disturbance due to the measurement can be conveniently described in terms of the following relations. If we obtain outcome A:

$$1 \sim \{1, 2\}, \quad 2 \sim \{1, 2\}, \quad 3 \sim \emptyset, \quad 4 \sim \emptyset \tag{2.32}$$

and if we obtain outcome B:

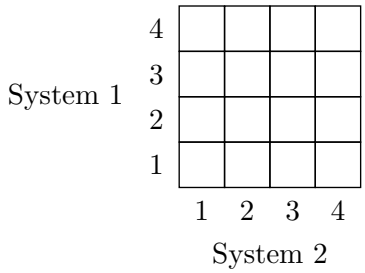
$$1 \sim \emptyset, \quad 2 \sim \emptyset, \quad 3 \sim \{3, 4\}, \quad 4 \sim \{3, 4\} \tag{2.33}$$

or more generally, if $\amalg_A, \amalg_B \subset \text{IV}$ correspond to outcomes A and B respectively, then if we get outcome A we apply $\amalg_A \sim \amalg_A, \amalg_B \sim \emptyset$ and similarly for outcome B.

The rules for probabilities of measurement outcomes and disturbance by measurement both indicate that the three families of epistemic states in diagram 2.27 constitute clear analogues of QM eigenstates for the three measurements depicted in diagram 2.29, and that furthermore the three measurements are not only incompatible, but mutually unbiased.

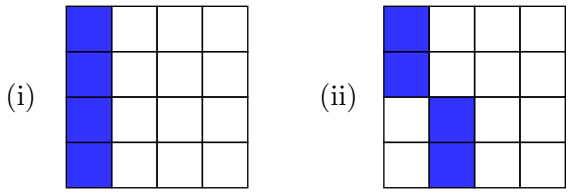
2.4.4 States of composite systems

The ontic state space for a pair of systems is IV × IV, thus there are sixteen possible ontic states, which correspond to every possible combination of the ontic states for the individual systems. We represent this state space in the following fashion:



(2.34)

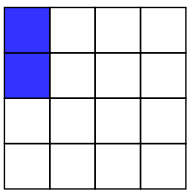
In this case a canonical question set contains four questions, since this is how many yes-no questions it takes to single out one ontic state from the sixteen. Thus, in an epistemic state of maximal knowledge we know that the ontic state is one of four possibilities. However, there are tighter requirements on the allowed epistemic states. For example, despite having the right number of filled boxes, the following two states are not allowed:



(2.35)

Our first extra requirement is that the knowledge balance principle should apply to each constituent system as well as to the overall composite system. This is where (i) fails, since if this is our epistemic state, we know for sure that system 2 is in ontic state 1.

Epistemic state (ii) satisfies the knowledge balance principle overall, and on all its subsystems. The problem here is that applying an allowed operation to this state will yield an epistemic state which doesn't satisfy the knowledge balance principle. Consider applying a measurement of the first type depicted in diagram 2.29, to system 1 of a pair of systems described by the epistemic state (ii). If we obtain outcome B, then, assuming that the disturbance induced by the measurement acts only on the measured system, the epistemic state after measurement will be:



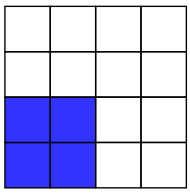
(2.36)

which fails to satisfy the knowledge balance principle either for system 2, or for the composite system as a whole.

We note in passing that the fact that the measurement disturbance only affects the measured system, and not any (potentially quite distant) other constituent systems is what makes the toy theory a *local* theory.

After applying such arguments as these, Spekkens shows that there are essentially two kinds of allowed epistemic states of maximal knowledge on a composite system of two elementary systems.

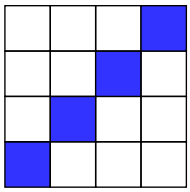
1. This state, and all states which can be obtained from it by permuting the rows and columns of the diagram:



(2.37)

   These are the analogues of the *separable* states of QM. In such states we have maximal knowledge about the individual systems, but we know nothing about the relationship between them. There are 36 such states in total.

2. This state, and all states which can be obtained from it by permuting the rows and columns of the diagram:



(2.38)

   These are the analogues of the *totally entangled* states of QM. In such states we know nothing about the individual systems, but we have full knowledge of the relationship between the systems. There are 24 such states in total.

There are further states, of non-maximal knowledge, which again play a role in the theory analogous to the mixed states of quantum mechanics.

We will not record all the details here (these can be found in the original paper [32]), but one can go on to develop the treatment of two-system transformations and measurements in a way very analogous to what was described for single systems. As was the case with the development of two-system states, there are extra complications which were not present for the single system case, but the essential principles are the same.

In his original paper Spekkens goes as far as treating the case of three systems. Here he determines that there are essentially three kinds of epistemic state: one in which there is no correlation between the three systems (essentially an extension of the type of state depicted in equation 2.37), one in which one system is uncorrelated with the other two, which are correlated, and one in which all three systems are correlated. Clearly it's harder to depict such states graphically, but an example of such a state would be the following subset of $\text{IV} \times \text{IV} \times \text{IV}$:

$$\{(1,1,1),(1,2,2),(2,1,2),(2,2,1),(3,3,3),(3,4,4),(4,3,4),(4,4,3)\} \tag{2.39}$$

These states are the analogues of the GHZ states of quantum mechanics.

Spekkens devotes considerable time to demonstrating that the properties of the states and transformations of the theory are such that many typically quantum phenomena are reproduced. Examples include the 'remote steering' effect, whereby given an entangled two-system state the choice of measurement on one system can 'steer' the other system into a state from a particular basis; the well-known dense-coding [7] and quantum teleportation [6] protocols; and the no-cloning [35] and no-broadcasting [2] results. Many of these results seem bizarre or inexplicable in the quantum context, but are seen to be quite trivial and comprehensible phenomena within the toy theory. For example the apparent teleportation of a whole state via the communication of just two bits, in the teleportation protocol is shown not to be at all mysterious when the state is a state of incomplete knowledge, rather than a quantum state. Perhaps the most notable quantum phenomena which are *not* reproduced are all the no-go results ruling out local hidden variables, for example violation of Bell inequalities. This is clearly to be expected, since the toy theory is a local hidden variable theory, by construction.

The toy theory clearly bears a very close resemblance to stabiliser theory: they both have one kind of elementary system, and discrete collections of states and transformations. In both cases the elementary system has three mutually unbiased observables, each with two outcomes. Evolution of the single system is described by a set of 24 transformations, together forming the group S_4. In both cases the 2-system states are either separable/totally uncorrelated, or maximally entangled/totally correlated. In fact we introduced the stabiliser theory precisely because it is the fragment of QM which the toy theory most closely resembles. However, despite their similarity they are clearly not quite the same, since the GHZ no-go proof shows that the results of the stabiliser theory could not be replicated by a local hidden variable theory.

2.4.5 Is the toy theory well-defined and consistent?

In his original paper Spekkens works out the details of the epistemic states and transformations in the theory up to the case of three systems. In later work he has extended this to four systems [31]. Nevertheless, the approach he takes to deriving the allowed epistemic states and transformations seems inevitably to be iterative, requiring derivation of states and transforms for systems with smaller numbers of components before those for systems with larger numbers of components can be determined.

The style of the original paper is quite informal, but essentially the procedure for determining allowed epistemic states and transformations for a system with n elementary components seems to amount to the following:

1. We first determine whether an epistemic state satisfies the knowledge balance principle 'globally' i.e. do we know the answer to half or less of a set of canonical questions about the system as a whole. In practice this means that allowed states constitute subsets of IV^n with one of the following cardinalities: $2^n, 2^{n+1}, \ldots, 2^{2n}$.

2. Clearly a system of n elementary components will have many possible subsystems: for example it will have n subsystems each with $n-1$ elementary components, $\frac{n(n-1)}{2}$ subsystems with $n-2$ elementary components, and so on, down to n subsystems each with one elementary component. Given an epistemic state for the full system, we

can clearly derive 'marginal' epistemic states on any of these subsystems: the original epistemic state is a subset of n-tuples, and we derive the 'marginal' state by deleting from each tuple the components corresponding to the elementary systems which do not appear in our subsystem of interest. Each of these marginal epistemic states must itself be a valid epistemic state. It was this requirement which failed to be satisfied for state (i) in diagram 2.35 in the previous section, thus ruling this out as a valid epistemic state. Note that this requirement requires knowledge of all allowed epistemic states for systems of $n-1, n-2, \ldots, 1$ elementary components.

3. The last rule is: Applying a valid operation to a valid epistemic state must yield a valid epistemic state. Spekkens employs this requirement on several occasions in his development of the theory. For example, having established the valid epistemic states of an elementary system in section 2.4.2 we used this rule in section 2.4.3 to deduce that the valid transformations on an elementary system were the permutations: any other transformations would have mapped valid states into non-valid states. Note that here we use our knowledge of valid states to deduce the form of the valid transformations. On the other hand, in ruling out state (ii) in diagram 2.35 in the previous section, we used our knowledge of the form of the valid transformation corresponding to measurement disturbance to deduce the form of valid states. Once again, using this rule requires us to have already deduced the valid form for certain states or transformations.

These appear to be the only rules which Spekkens uses in deriving the form of allowed states and transformations, although their application is something of an art! They raise several issues. Firstly, this approach seems to be necessarily iterative. Compare it for example to how we would describe the form of valid states in quantum mechanics - in one line we can say that they are the normalised vectors of the system's state space.

Secondly, do these rules actually uniquely define the toy theory? There does seem to be a problem with the third rule. When we use it to rule out state (ii) in diagram 2.35, our argument is that we already know what the valid measurement disturbance transformations on a single elementary system are, and when we apply one of them to state (ii) we obtain a state which clearly violates the knowledge balance principle. However, it is not clear that we could not have made the alternative choice - that this state should be valid, and therefore that the transformation which we had previously thought was valid could no longer be considered as such. It seems that considerations other than the three rules above come into deciding which should be the valid states of the theory, but it is nowhere clearly stated exactly what they are.

The second point touched slightly on our final issue: is the theory as Spekkens presents it consistent? He derives valid states and transformations for systems with up to three elementary components. However, can we be sure that these states and transformations, when combined in more complex situations involving four or more elementary systems, won't yield a state which clearly violates the knowledge balance principle? Currently there seems to be no such proof of consistency. In fact, on the way to deriving a categorical treatment of the theory we will develop such a proof. This will be discussed further in chapter 4.

Chapter 3

Background: the categorical framework

In this section we introduce the programme initiated by Abramsky and Coecke [1] and continued by many authors, for example [29, 13, 9], to re-express quantum mechanics and quantum-like theories in terms of category theory. This programme has had multiple motivations, which have been more or less important to different authors. In this work we will primarily view the categorical approach as a unifying mathematical framework in which to study and compare quantum-like theories which were originally expressed in disparate mathematical forms.

The key idea in the categorical approach is to concentrate on the 'algebra' of how operations and transformations of systems in a theory combine. Two physical theories might represent their states and operations using quite different mathematical structures, but in the categorical approach we are uninterested in the 'internal structure' of states and operations. Instead we view the operations as the primitive mathematical elements, and ask how they combine. For example, if I perform operation A, followed by operation B, and the overall result is the same as if I had simply performed the operation C, then we can form an equation on our operations: $A;B = C$. We will now see that categories are the appropriate mathematical arena for stating such results.

In section 3.1 we introduce the basic category theoretic definitions, and discuss why categories are the appropriate structure with which to model the algebra of processes in a physical theory. We introduce a particular type of category, a *symmetric monoidal category* and show that any category corresponding to a physical theory will be of this type. In section 3.2 we introduce some additional structures which we expect any category corresponding to a *quantum-like* theory to possess. We continue with this in section 3.3 which is devoted to a structure which will be of particular importance in succeeding chapters, the *basis structure*. Finally in section 3.4 we give a detailed description of the category **Stab**, which corresponds to the stabiliser theory described in the previous chapter.

Since this chapter primarily summarises an existing body of work for the most part we will state results without proof. Details of proofs can be found in the references. The definition of **Stab** first appeared in a paper co-authored with Bob Coecke and Rob Spekkens [11].

3.1 Categories and physical theories

3.1.1 Basic definitions in category theory

A category [23] is an algebraic structure like a group, a field or a vector space. A category is a collection of elements with an associative binary operation, but, unlike the examples above, this operation is not defined for all pairs of elements. Each element has a pair of labels which determine which other elements it can combine with. For example an (A, B) element can combine with a (B, C) element; the result will be an (A, C) element, which could then combine with a (C, D) element to produce an (A, D) element, or could combine with a (Z, A) element to yield a (Z, C) element. The order of the labelling is important: a (B, A) element could not combine with a (B, C) element. Thus each element has a kind of inherent 'direction', and they are often termed *arrows*.

This is not the standard way of introducing a category, though it has the merit of emphasising exactly where the algebraic structure of the category lies. A more standard definition is:

Definition 3.1.1 A *category* $\mathcal{C}$ consists of:

- A collection of **Objects**, denoted $\mathrm{Ob}(\mathcal{C})$. These are normally labelled $A, B, C, \ldots$. These are not the algebraic elements of the system, they are the labels referred to above.
- A collection of **Arrows** or **Morphisms**, denoted $\mathrm{Hom}(\mathcal{C})$ to each of which are associated two objects, one called the *domain* of the morphism, the other its *codomain*. The morphism f with domain A and codomain B would be written as $f : A \to B$ or $A \xrightarrow{f} B$. We also write $f \in \mathcal{C}(A, B)$. These morphisms are the algebraic elements of the category.

Furthermore, for each triple of objects A, B and C there is a map $c_{A,B,C} : \mathcal{C}(A, B) \times \mathcal{C}(B, C) \to \mathcal{C}(A, C)$. Given $f : A \to B$ and $g : B \to C$ we denote $c_{A,B,C}(f, g)$ by either $g \circ f$ or $f; g$. This operation satisfies two conditions:

- It is associative: $(h \circ g) \circ f = h \circ (g \circ f)$
- Each object A has an associated identity morphism, denoted id_A or 1_A so that if $f : A \to B$ then $f \circ 1_A = f = 1_B \circ f$.

Definition 3.1.2 A *sub-category* $\mathcal{C}'$ of a category $\mathcal{C}$ consists of:

- A sub-collection of the objects of $\mathcal{C}$, $\mathrm{Ob}(\mathcal{C}') \subseteq \mathrm{Ob}(\mathcal{C})$.
- A sub-collection of the morphisms of $\mathcal{C}$, $\mathrm{Hom}(\mathcal{C}') \subseteq \mathrm{Hom}(\mathcal{C})$.

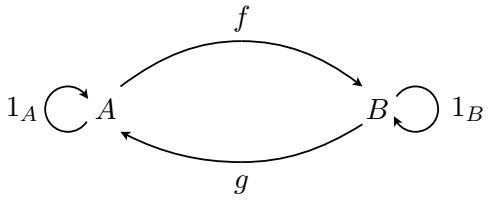
such that

- $\forall A \in \mathrm{Ob}(\mathcal{C}')$, $1_A \in \mathrm{Hom}(\mathcal{C}')$.

- $\forall f : A \to B \in \mathrm{Hom}(\mathcal{C}')$, $A, B \in \mathrm{Ob}(\mathcal{C}')$.
- $\forall f : A \to B, g : B \to C \in \mathrm{Hom}(\mathcal{C}')$, $g \circ f \in \mathrm{Hom}(\mathcal{C}')$.

3.1.2 Examples of categories; link to physical theories

Concrete realisations of categories take many forms. We can construct very simple abstract structures, satisfying the axioms of a category, unrelated to any other context. For example, the following diagram illustrates a very simple category with two objects:



(3.1)

where: $g \circ f = 1_A$ and $f \circ g = 1_B$.

However, concrete examples of categories also arise naturally in other contexts. The notation $f : A \to B$ is clearly reminiscent of the notation for functions and sets, and this is no coincidence. Some of the most important concrete examples of categories are those in which the objects are some form of mathematical structure, and the arrows are maps which preserve this structure. Key examples include:

- **Set** in which the objects are sets, and the arrows are functions.
- **Grp** in which the objects are groups and the arrows are group homomorphisms.
- **Rel** in which the objects are sets, and the arrows are relations.
- **Hilb** in which the objects are Hilbert spaces and the arrows are linear maps.

It is straightforward to verify in each case that the objects and arrows obey the axioms of a category. In each case we are uninterested in the internal structure of the objects, we are interested in the algebra of how the morphisms combine. For example, although the objects of **Set** and **Rel** are the same, as categories they have very different structures; in fact **Rel** has much more in common with **Hilb** than it does with **Set**.

It is clear that any physical theory will also give rise to a category, whose objects are the systems of the theory, and whose arrows are the operations or transformations which these systems can undergo. Such a 'physical' category is of course always going to be isomorphic to a 'mathematical structure' category of the type described in the previous paragraph. This is because the states of the systems in a theory are described by some sort of element in a mathematical structure, and the operations which transform these states essentially map one such state element into another.

Definition 3.1.3 The *physical category* of a theory is the category whose objects are the mathematical structures whose elements are used by the theory to describe states of systems, and whose morphisms are the structure preserving maps used by the theory to represent transformations of systems.

Some examples will make this clear:

Example 3.1.4 In pure state quantum mechanics the state of a system is described by a vector in a Hilbert space. Via carefully chosen operations, it is actually possible to realise every linear map as a transformation on states [17]. Thus the physical category of pure state quantum mechanics (the form of QM which we will concentrate on in this work), is **FHilb**, whose objects are finite-dimensional Hilbert spaces and whose arrows are linear maps.

Example 3.1.5 The states in Spekkens's toy theory are subsets of state space, and the most general form of transformations these states can undergo are described by relations between the sets. Thus it is unsurprising that the toy theory's physical category, **Spek**, is a subcategory of the category **FRel** whose objects are finite sets and whose arrows are relations. **Spek** will be formally defined, and its properties extensively analysed in chapter 4.

3.1.3 Further concepts in category theory

Before proceeding further we need to introduce a few more categorical concepts. Firstly, we note that categorical equations are often expressed with the aid of *commutative diagrams*. For example, given four morphisms $f : A \to B$, $g : B \to D$, $h : A \to C$ and $k : C \to D$, the commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{k} & D \end{array} \tag{3.2}$$

expresses the equation $g \circ f = k \circ h$. Although this notation seems to provide no advantage in this simple case, this kind of diagram can be very helpful in clarifying complex equations.

Next we introduce structure preserving maps between categories:

Definition 3.1.6 A *functor* F between categories $\mathcal{C}$ and $\mathcal{D}$, denoted $F : \mathcal{C} \to \mathcal{D}$, is a pair of functions, $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ and $F : \mathrm{Hom}(\mathcal{C}) \to \mathrm{Hom}(\mathcal{D})$ such that:

- $\forall A, B \in \mathrm{Ob}(\mathcal{C}), f \in \mathrm{Hom}(\mathcal{C})$, if $f \in \mathcal{C}(A, B)$ then $F(f) \in \mathcal{D}(F(A), F(B))$.
- $F(g \circ f) = F(g) \circ F(f)$; $F(1_A) = 1_{F(A)}$

We also define what is effectively a map between functors:

Definition 3.1.7 Given two functors $F, G : \mathcal{C} \to \mathcal{D}$, a *natural transformation* $\theta : F \to G$ exists iff $\forall A \in \mathrm{Ob}(\mathcal{C})$ there exists a morphism $\theta_A : F(A) \to G(A) \in \mathrm{Hom}(\mathcal{D})$ such that the

following diagram commutes:

$$\begin{array}{ccc} F(A) & \xrightarrow{\theta_A} & G(A) \\ \Big\downarrow{\scriptstyle F(f)} & & \Big\downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow{\theta_B} & G(B) \end{array} \tag{3.3}$$

for all pairs of objects $A, B \in \mathrm{Ob}(\mathcal{C})$ and all morphisms $f \in \mathcal{C}(A, B)$.

Definition 3.1.8 Two morphisms $f : A \to B$ and $g : B \to A$ are *isomorphisms* iff $g \circ f = 1_A$ and $f \circ g = 1_B$. g is often written as f^{-1}. Two objects A and B are *isomorphic* iff there exists a pair of isomorphisms between them.

3.1.4 Symmetric monoidal categories

A symmetric monoidal category (SMC) is a type of category obeying additional conditions. Such categories are of particular interest to us because all physical categories are SMCs. In any physical theory we can consider two or more systems as one single composite system. Thus the corresponding physical category must have some operation whereby two objects can be combined together to yield a third object. Given a composite system, we can perform independent operations on the constituent parts: these 'parallel' operations can be seen as a single operation on the composite system. Thus, the operation of combining physical systems must extend beyond objects and apply to morphisms as well. We expect then that a physical category will have some sort of functor-like operation corresponding to forming a composite system. Naturally this operation will be bound by various restrictions. We will first define the kind of structure required, and then return to show that it does indeed correspond to the physical idea of compositeness.

Definition 3.1.9 A *symmetric monoidal category* $(\mathcal{C}, I, - \otimes -)$ is a category equipped with the following extra structure:

- A bifunctor $- \otimes - : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$. (Bifunctoriality means that $(f_2 \circ f_1) \otimes (g_2 \circ g_1) = (f_2 \otimes g_2) \circ (f_1 \otimes g_1)$).
- A *unit object* I.
- Four natural isomorphisms, left and right unit:

$$\lambda_A : A \cong I \otimes A \qquad \rho_A : A \cong A \otimes I \tag{3.4}$$

  associative:

$$\alpha_{A,B,C} : (A \otimes B) \otimes C \cong A \otimes (B \otimes C) \tag{3.5}$$

  and commutative:

$$\sigma_{A,B} : A \otimes B \cong B \otimes A \tag{3.6}$$

Furthermore these objects and natural isomorphisms obey a series of *coherence conditions* [23].

Example 3.1.10 Both $(\mathbf{Set}, \{*\}, - \times -)$ and $(\mathbf{Set}, \emptyset, - \sqcup -)$ are SMCs. This demonstrates that the same underlying category with different choices of monoidal bifunctor and unit object can give rise to different SMCs.

Example 3.1.11 Both $(\mathbf{FRel}, \{*\}, - \times -)$ and $(\mathbf{FRel}, \emptyset, - \sqcup -)$ are SMCs.

Example 3.1.12 Both $(\mathbf{FHilb}, \mathbb{C}, - \otimes -)$ and $(\mathbf{FHilb}, \mathbf{0}, - \oplus -)$, where $\mathbf{0}$ is the zero-dimensional vector space consisting solely of the zero vector, are SMCs. It is the first of these which is the physical category for pure state quantum mechanics.

For the remainder of this work, unless otherwise stated, when we refer to the SMCs **FRel** and **FHilb** we mean the first of the two SMCs in each of the above examples.

Definition 3.1.13 In a SMC a *scalar* is a morphism of type $I \to I$.

Proposition 3.1.14 $(\mathcal{C}(I, I), - \circ -, 1_I)$ is a commutative monoid.

Example 3.1.15 The scalars of **FHilb** are $\mathbb{C}$. The scalars of **FRel** are the elements of the two element Boolean algebra $\mathbb{B}_2$.

We can define an abstract notion of scalar multiplication, whereby we can multiply any morphism by a scalar:

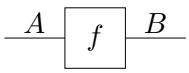
Definition 3.1.16 Scalar multiplication of a morphism $f : A \to B$ by a scalar $s : I \to I$ is defined by:

$$\begin{array}{ccc} A & \xrightarrow{s \bullet f} & B \\ {\scriptstyle \lambda_A}\downarrow & & \uparrow{\scriptstyle \lambda_B^{-1}} \\ I \otimes A & \xrightarrow{s \otimes f} & I \otimes B \end{array} \tag{3.7}$$

There is an extremely useful graphical language for describing SMCs. In this language we represent an object A by a labelled line:

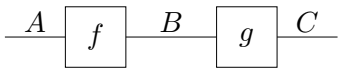
$$\underline{\qquad A \qquad} \tag{3.8}$$

and we represent a morphism $f : A \to B$ by a box:



(3.9)

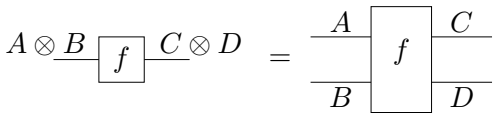
$g \circ f$, the composition of morphisms $f : A \to B$ and $g : B \to C$ is depicted as:



(3.10)

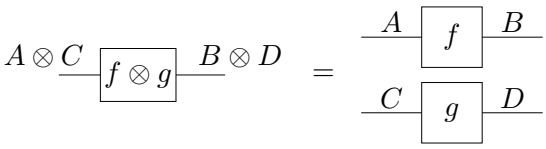
The identity morphism 1_A is actually just written as a straight line — this makes sense if you imagine composing it with another morphism.

Turning to the symmetric monoidal structure, a morphism $f : A \otimes B \to C \otimes D$ is depicted:



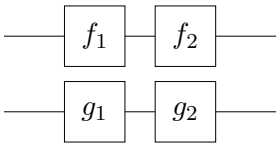
(3.11)

and if $f : A \to B$ and $g : C \to D$ then $f \otimes g$ is depicted as:



(3.12)

Note that bifunctoriality is implicit in this language: $(f_2 \circ f_1) \otimes (g_2 \circ g_1)$, and $(f_2 \otimes g_2) \circ (f_1 \otimes g_1)$, equated by bifunctoriality, are both written as:

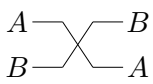


(3.13)

The identity object I is not actually depicted in the graphical language. Morphisms $\psi : I \to A$ and $\pi : A \to I$ are written as:

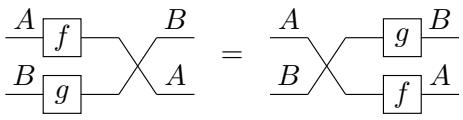
(3.14)

The associativity and left and right unit natural isomorphisms are also implicit in the language. The symmetry natural isomorphism is depicted as:



(3.15)

The fact that it is a natural transformation depicts as:



(3.16)

In fact the graphical language is more than just a useful tool - it is completely equivalent to the axioms of a SMC:

Theorem 3.1.17 Two morphisms in a symmetric monoidal category can be shown to be equal using the axioms of a SMC iff the diagrams corresponding to these morphisms in the graphical language are isomorphic as graphs.

Proof: This important theorem is proved in [20]. □

This graphical language is very suggestive of the physical interpretation of SMCs, which was the original motivation for introducing this type of category. We return to this subject and note that the operation of combining systems naturally has all of the properties of the bifunctor of a SMC.

Forming a composite system is clearly an associative operation, and it would be a very odd physical theory for which it was not also a commutative one. It turns out to be convenient to have an object to represent the *absence* of a system, and the monoidal unit object has exactly the properties we would expect from such an object.

The action of the bifunctor on the morphisms is also bound by the kind of conditions we would expect given the physical interpretation. The bifunctoriality condition itself (shown in diagram 3.13) is trivially true when we view the morphism $f \otimes g$ as two independent operations f and g on separate systems. The naturality of the isomorphisms in equations 3.4 to 3.6 also has a clear physical interpretation. For example, consider the naturality of the symmetry isomorphism, as depicted graphically in diagram 3.16. Informally what this depicts is: system A starts on my left, system B on my right. I perform operation f on the left hand system and g on the right hand system. Then I swap the two systems around. This is the same as swapping the two systems first, and then performing g on the left hand system and f on the right hand system. This is obviously what we expect!

In a physical category the special object I represents the absence of a system. This allows us to describe *preparations*, processes in which a new system is created: these are morphisms from I to the object representing the new system. There may be several such arrows, e.g.

$$\psi : I \to A \text{ and } \phi : I \to A$$

are different ways of preparing the system A, i.e. they represent preparing A in two different states. Morphisms of type $I \to A$ in physical categories will, for this reason, frequently be described as *states*. Morphisms of type $A \to I$ will be termed *co-states*.

Remark 3.1.18 The states of **FRel** are relations of type $R : \{*\} \to X$. It is clear that these relations are in bijection with the subsets of X, and in what follows we often (somewhat abusively) work as if the states of **FRel** *are* subsets.

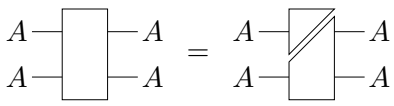
Remark 3.1.19 In example 3.1.12 it was noted that in **Hilb** the role of I is played by $\mathbb{C}$. It may not be immediately obvious that operators of the form $\psi : \mathbb{C} \to \mathcal{H}$ represent preparations of systems in certain states. However, note that the linear maps from $\mathbb{C}$ to $\mathcal{H}$ are in bijective correspondence with the vectors in $\mathcal{H}$. This is because the action of a *map* $\psi : \mathbb{C} \to \mathcal{H}$ is entirely determined by its action on 1, because of its linearity: if $c \in \mathbb{C}$ then $\psi(c) = c\psi(1)$. So each function $\psi : \mathbb{C} \to \mathcal{H}$ corresponds to a particular vector in $\mathcal{H}$. In the standard formulation of QM each vector in $\mathcal{H}$ represents a state of the system. So, the operations $\psi : \mathbb{C} \to \mathcal{H}$ are exactly able to describe preparations of the system in all of its possible states.

Some readers might argue, with some justification, that an operation of type $I \to A$, where we simply create a system out of nothing, does not exist in any theory that actually describes the real world. Such an operation would seem to defy the conservation of mass for example. This is a good point to clarify what exactly the morphisms in the physical category of a theory represent.

If one straightforwardly views the morphisms in a physical category as representing physical processes, then a morphism $f : A \to B$ transforms one system into another, perhaps turning an electron into a proton. A morphism $\delta : A \to A \otimes A$ takes one system, and electron perhaps, and turns it into two electrons. Putting aside quantum field theory, it is hard to see how these sort of processes can occur in the physical theories we are familiar with (for example QM), and yet the categorical approach is claiming that they occur in the corresponding physical categories, and furthermore (as we will see) are important.

Conceivably these operations could form part of a theory describing one open subsystem of a larger closed system. The preferred interpretation of this author however, is that the morphisms of a physical category do not necessarily individually represent realisable processes in the corresponding theory, rather they represent patterns of dependency or information flow.

For example, consider a system of two electrons. These electrons may undergo a process which changes their state. So long as we remain within standard non-relativistic QM, this process will not result in any final system other than the same two electrons we began with. However, it may well be that the final state of the two electrons depends only on the initial state of one of the electrons, with the initial state of the other electron having no influence on the final state of either. In this case we could decompose the process into two parts, illustrated diagrammatically here:



(3.17)

one of type $A \to I$, the other of type $A \to A \otimes A$. It is quite reasonable to claim that the theory corresponding to our physical category includes both of these operations, even if it is impossible, in practice, to realise them individually. In fact, it is a key claim of the categorical approach that an analysis of these types of operation is enlightening, and yields fresh insight into the theory under consideration.

3.2 Physical categories of quantum-like theories

Our particular interest is quantum mechanics, and other quantum-like theories which share certain features with QM. Thus, from a categorical perspective, we are interested in a particular class of physical categories. Over the next few sections we will identify categorical features of **FHilb** which are important in its description of QM, which we expect to recur in the physical categories of other quantum-like theories. Much of this material will initially appear to have little physical relevance, but it is all essential background to what follows.

3.2.1 Dagger categories

Any linear map $f : \mathcal{H}_1 \to \mathcal{H}_2$ on a Hilbert space has an *adjoint* or *Hermitian conjugate*, $f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1$, defined using the inner product by:

$$\langle \phi | f\psi \rangle = \langle f^\dagger \phi | \psi \rangle \tag{3.18}$$

It's simple to show that the adjoint satisfies several important properties: for example $(f^\dagger)^\dagger = f$, $(f \circ g)^\dagger = f^\dagger \circ g^\dagger$ etc. It will turn out to be useful to abstract some of the features of the adjoint to a more general categorical setting:

Definition 3.2.1 A *dagger category* is a category, $\mathcal{C}$, equipped with a functor $(-)^\dagger$ which is:

- **Identity on Objects**: $A^\dagger = A$
- **Contravariant**: a contravariant functor F reverses the direction of arrows i.e. if $f : A \to B$ then $Ff : FB \to FA$. So in this case $f^\dagger : B^\dagger \to A^\dagger$. But since $A^\dagger = A$ in fact we have $f^\dagger : B \to A$.
- **Involutive**: $(f^\dagger)^\dagger = f$

Remark 3.2.2 Because of these properties we note that the dagger functor induces a bijection between the hom-sets $\mathcal{C}(A, B)$ and $\mathcal{C}(B, A)$. From this we can immediately see that **Set** cannot be a dagger category, because in general there is no such bijection between hom-sets. To see this consider the hom-set of functions from the singleton set to an n-element set, $\mathbf{Set}(\{*\}, N)$ which has n members, and contrast it with this hom-set $\mathbf{Set}(N, \{*\})$ which has just one member. In contrast, **Rel** is a dagger category, with relational converse as the dagger operation.

If a category is also a SMC, then we are interested to see how the dagger and symmetric monoidal structures interact. They interact most 'neatly' in the following case:

Definition 3.2.3 A *dagger symmetric monoidal category* (†-SMC) is a symmetric monoidal category with a dagger functor such that:

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger \text{ and} \tag{3.19}$$

$$\lambda_A^{-1} = \lambda_A^\dagger \qquad \rho_A^{-1} = \rho_A^\dagger \tag{3.20}$$

$$\sigma_{A,B}^{-1} = \sigma_{A,B}^\dagger \qquad \alpha_{A,B,C}^{-1} = \alpha_{A,B,C}^\dagger \tag{3.21}$$

Example 3.2.4 $(\mathbf{FRel}, \{*\}, - \times -)$ is a †-SMC with the relational converse playing the role of the dagger functor.

Example 3.2.5 $(\mathbf{FHilb}, \mathbb{C}, - \otimes -)$ is a †-SMC with the adjoint playing the role of the dagger functor.

The physical significance of the dagger functor will become clearer once we introduce the abstract equivalent of observables. At this stage the key feature is the bijection between hom-sets noted in remark 3.2.2, which will be an important ingredient in subsequent definitions.

3.2.2 Compact closed categories

There is a second important bijection amongst the morphisms of **FHilb**, this time between maps of type $\mathcal{H}_A \to \mathcal{H}_B$, and bipartite states, of type $I \to \mathcal{H}_A \otimes \mathcal{H}_B$.

The most general vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written as:

$$|\psi\rangle = \sum_{i,j} \psi_{ij} |a_i\rangle_A \otimes |b_j\rangle_B \tag{3.22}$$

where the $|a_i\rangle_A$ are a basis for $\mathcal{H}_A$ and the $|b_j\rangle_B$ are a basis for $\mathcal{H}_B$, and the ψ_{ij} are complex numbers. The most general linear map $f : \mathcal{H}_A \to \mathcal{H}_B$ can be written as:

$$f = \sum_{i,j} f_{ji} |b_j\rangle_B \, {}_A\langle a_i| \tag{3.23}$$

where the f_{ji} are complex numbers. Clearly the possibilities for ψ_{ij} and f_{ji} are in bijective correspondence. There is a *map-state duality* in **FHilb**. The state $|\psi\rangle$ and map f for which $\psi_{ij} = f_{ji} = M_{ij}$ are dual.

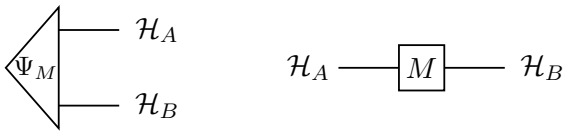
Given a Hilbert space $\mathcal{H}_A$ and a choice of basis vectors $|a_i\rangle_A$, consider the following (non-normalised) state and co-state:

$$\begin{array}{ll} |\Psi_{\text{Bell}}\rangle = & \sum_i |a_i\rangle \otimes |a_i\rangle \\ \langle\Psi_{\text{Bell}}| = & \sum_i \langle a_i| \otimes \langle a_i| \end{array} \tag{3.24}$$

Considered as morphisms in **FHilb** these have types $I \to \mathcal{H}_A \otimes \mathcal{H}_A$ and $\mathcal{H}_A \otimes \mathcal{H}_A \to I$, respectively, and we *provisionally* depict them in the graphical language as follows:

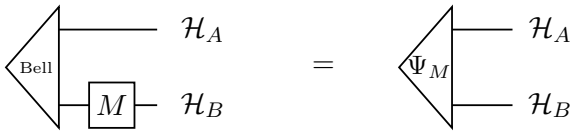
(3.25)

Now consider a state, $|\Psi_M\rangle = \sum_{i,j} M_{ij}|a_i\rangle_A \otimes |b_j\rangle_B$ and map $M = \sum_{i,j} M_{ij}|b_j\rangle_B\,{}_A\langle a_i|$, clearly dual in the sense described above, and depicted graphically as:



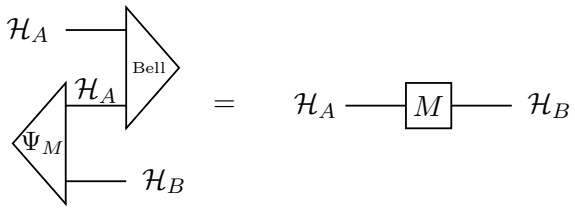
(3.26)

Now consider composing M with $|\Psi_{\text{Bell}}\rangle$ as shown in the diagram below. A simple calculation shows that this is equal to $|\Psi_M\rangle$:



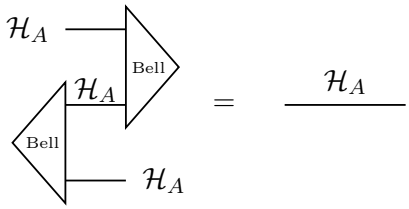
(3.27)

Likewise consider composing $|\Psi_M\rangle$ with $|\Psi_{\text{Bell}}\rangle$. Again, a simple calculation shows that this is equal to M:



(3.28)

So these two morphisms in equation 3.24 provide a compositional way of moving between states and maps. In fact a closer inspection of the linear algebra calculations which underlie the graphical equations 3.27 and 3.28 shows that they basically arise from a more fundamental relationship, shown graphically here:



(3.29)

Equally if we begin with this fact, then we can treat either 3.27 or 3.28 as a definition, and derive the other.

This 'compositionally derived' bijection between hom-sets is another feature of **FHilb** which it will be convenient to abstract to the more general categorical setting, and to this end we introduce the following definitions:

Definition 3.2.6 In a SMC $\mathcal{C}$ a *compact structure* on an object A is a tuple $\{A, A^*, \eta_A : I \to A^* \otimes A, \epsilon_A : A \otimes A^* \to I\}$, where A^* is a dual object to A which may or may not be equal to

A, and η_A and ϵ_A satisfy the conditions:

$$\begin{array}{ccccc} A & \xrightarrow{\rho_A} & A \otimes I & \xrightarrow{1_A \otimes \eta_A} & A \otimes (A^* \otimes A) \\ \downarrow{\scriptstyle 1_A} & & & & \downarrow{\scriptstyle \alpha_{A,A^*,A}} \\ A & \xleftarrow{\lambda_A^{-1}} & I \otimes A & \xleftarrow{\epsilon_A \otimes 1_A} & (A \otimes A^*) \otimes A \end{array} \tag{3.30}$$

and the dual diagram for A^*.

Definition 3.2.7 A *compact closed* category $\mathcal{C}$ is a SMC in which all $A \in \mathrm{Ob}(\mathcal{C})$ have compact structures.

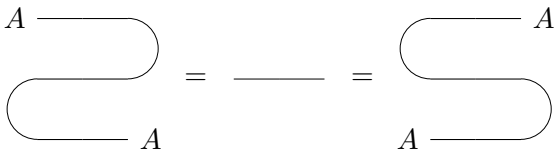
Example 3.2.8 In **FHilb** we can assign $\mathcal{H}_A^* = \mathcal{H}_A$, and $\eta_{\mathcal{H}_A} = |\Psi_{\mathrm{Bell}}\rangle$ and $\epsilon_{\mathcal{H}_A} = \langle\Psi_{\mathrm{Bell}}|$, as defined in equation 3.24. The commutative diagram 3.30 translates into the wire diagram 3.29.

All of the compact structures with which we will be dealing in this work will be self-dual, i.e. $A^* = A$. For a more general treatment of compact closure in categorical quantum mechanics, where we do not assume self-duality see [1], [29].

Diagram 3.29 uses the graphical language introduced in section 3.1.4 along with the symbols introduced in equation 3.25 to depict the unit and co-unit. However, in view of the importance of these morphisms we will extend the graphical language by introducing special elements to represent them:

(3.31)

Equation 3.30 and its dual are then depicted as:



(3.32)

This extension of the graphical language now renders it completely equivalent to the axioms of a compact closed category.

Theorem 3.2.9 Two morphisms in a compact closed category can be shown to be equal using the axioms of compact closure iff the diagrams corresponding to these morphisms in the graphical language are isomorphic as graphs.

Proof: This important theorem is proved in [21]. □

Compact structures are not usually unique as the following proposition shows.

Proposition 3.2.10 Given a self-dual compact structure $\{A, A, \eta_A, \epsilon_A\}$, and an isomorphism $f : A \to A$, we can derive another compact structure $\{A, A, (1_A \otimes f) \circ \eta_A, (f^{-1} \otimes 1_A) \circ \epsilon_A\}$. Diagrammatically our new unit and co-unit are depicted as:

(3.33)

If we allow the domain and codomain of f to differ i.e. $f : A \to B$ then we can actually derive compact structures which are not self-dual. For such a structure $B = A^*$.

In general then, an object A will have many compact structures.

Example 3.2.11 Consider the state and co-state in equation 3.24, which constitute the unit and co-unit of a compact structure in **FHilb**. In general a different choice of basis vectors $|a_i\rangle$ will yield a different state $|\Psi_{\text{Bell}}\rangle$. This suggests that the duality in **FHilb** between maps of type $\mathcal{H}_A \to \mathcal{H}_B$ and states of type $I \to \mathcal{H}_A \otimes \mathcal{H}_B$ is basis-dependent, which is indeed the case.

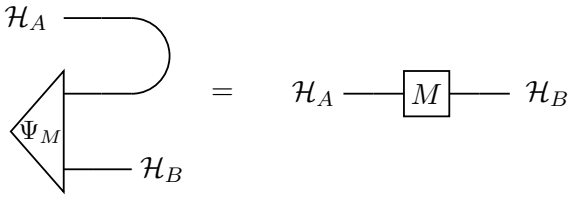
Note that this plurality of compact structures on A does pose some problems for our graphical language. If we use the diagrams in equation 3.31 it is not clear which of the many compact structures A they represent. Unless it is clear from the context, we must state explicitly which compact structure is represented by these wire diagrams.

Compact closure is an important structure in our study of quantum-like physical categories for several reasons. Firstly, we expect the physical categories of most quantum-like theories to be compact closed, since the unit/co-unit structure can actually arise from a more basic piece of structure, which, as we will see, models the essential features of quantum observables. We have chosen to discuss compact closure first so that when it arises in the context of basis structures (section 3.3.2) its full significance can be understood.

Secondly, compact closure has a direct physical interpretation. In the case of **FHilb** the unit corresponds to preparation of a Bell state. The 'compact closed derived' ability of Bell states to encode a linear transformation as a state is at the root of several important quantum information protocols, for example quantum teleportation [6], logic gate teleportation [17] and entanglement swapping [36]. Any physical category which is compact closed also has a state with these abilities and thus its corresponding theory shares with quantum mechanics the possibility of realising these protocols. The analysis of these protocols in abstract terms was one of the key initial motivations for the development of the categorical approach [1].

The third reason is probably the most important from our perspective. In any compact closed category there will be map-state duality, effectively of the type described at the start of this section: there will be a bijection between the hom-sets $\mathcal{C}(I, A \otimes B)$ and $\mathcal{C}(A, B)$ (in fact both these will further be in bijection with $\mathcal{C}(A \otimes B, I)$). Pairs of morphisms will be related by the

abstract equivalents of equations 3.27 and 3.28:

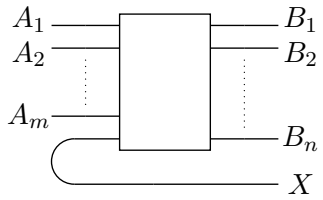


(3.34)

and

(3.35)

If we have a morphism with larger composite domain and codomain the number of hom-sets in bijection increases dramatically. For example the morphisms of the hom-sets $\mathcal{C}(A_1 \otimes \cdots \otimes A_m \otimes X, B_1 \otimes \cdots \otimes B_n)$ and $\mathcal{C}(A_1 \otimes \cdots \otimes A_m, B_1 \otimes \cdots \otimes B_n \otimes X)$ are in bijection: explicitly the conversion between morphisms from the two sets can be depicted as:



(3.36)

Clearly manoeuvres like this can convert any 'input' line into an 'output' line, by using the unit and co-unit morphisms to 'bend lines around'. The property of two morphisms being related via compact-closed duality is clearly an equivalence relation, which partitions the morphisms of a compact-closed category into classes.

Definition 3.2.12 A *diagram equivalence class* (DEC) is a set of morphisms in a compact closed category which can be inter-converted by composition with the units and co-units of the factors of their domains and codomains.

The terminology is inspired by the fact that the diagrams of all members of a class are essentially the same, only differing in the orientations of their input and output arrows. The idea of a DEC can be useful when working with the concrete representations of categories. When doing calculations with a morphism it may be more convenient to work with another member from its diagram equivalence class with a different type, and then translate the results back to the original type. We will use this procedure extensively in the next chapter.

It's important to note that DECs are defined *relative to a particular choice of compact structure for each object.*

A compact closed category may also have a dagger functor, this is clearly the case with **FHilb**. In **FHilb** the two structures work together nicely in a way which we formalise here:

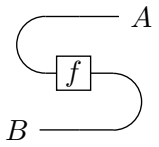
Definition 3.2.13 A *dagger compact closed category* is a compact closed category $\mathcal{C}$ with a dagger functor such that for all $A \in \mathrm{Ob}(\mathcal{C})$, $\eta_A = \sigma_{A,A^*} \circ \epsilon_A^\dagger$.

Finally we note that compact structures allow us to define some new operations on morphisms, which, if the category is compact closed, extend to functors on the whole category.

Definition 3.2.14 In a compact closed category we define the *upper star* operation on a morphism $f : A \to B$ by:

$$f^* = (1_A \otimes \epsilon_B) \circ (1_A \otimes f \otimes 1_B) \circ (\eta_A \otimes 1_B) : B \to A \tag{3.37}$$

or diagrammatically:



(3.38)

Note that the upper star operation is defined relative to a particular choice of compact structure on each object. Different choices of compact structure will yield a different upper star operation. This is illustrated in the next example:

Example 3.2.15 In **FHilb**, suppose our unit on a space A is given by the Bell state $|\Psi^A_{\text{Bell}}\rangle = \sum_i |a_i\rangle \otimes |a_i\rangle$ and our unit on B is given by the Bell state $|\Psi^B_{\text{Bell}}\rangle = \sum_i |b_i\rangle \otimes |b_i\rangle$, then the matrix representation of f^* *with respect to the bases* $|a_i\rangle$ *on* A *and* $|b_i\rangle$ *on* B is equal to the *transpose* of the matrix representation of f with respect to the same basis. It is well-known that the transpose of a linear map, unlike its adjoint, is a basis-dependent notion.

Proposition 3.2.16 The operation $(-)^*$ constitutes an identity-on-objects contravariant functor.

In a dagger compact closed category we can go further.

Proposition 3.2.17 In a dagger compact closed category, for any morphism $f : A \to B$, $(f^\dagger)^* = (f^*)^\dagger$.

Definition 3.2.18 In a dagger compact closed category we define the *lower star* operation on a morphism $f : A \to B$ by $f_* := (f^\dagger)^* = (f^*)^\dagger : A \to B$.

Clearly, since this operation is the result of applying one functor after another, it too is a functor:

Proposition 3.2.19 The operation $(-)_*$ constitutes an identity-on-objects covariant functor.

Again, the lower star operation is defined relative to a particular choice of compact structure on each object.

Example 3.2.20 In **FHilb**, suppose our units on A and B are those described in example 3.2.15, then the matrix representation of f_* *with respect to the bases* $|a_i\rangle$ *on* A *and* $|b_i\rangle$ *on* B is equal to the *complex conjugate* of the matrix representation of f with respect to the same basis. Again, complex conjugation is a basis-dependent notion.

3.2.3 Zero morphisms

Given any pair of Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ there exists a linear map $0_{1,2} : \mathcal{H}_1 \to \mathcal{H}_2$ such that $\forall \psi \in \mathcal{H}_1$, $0_{1,2}(\psi) = \mathbf{0}$. In quantum mechanics such maps are interpreted as 'impossible' operations, those which have zero probability of occurring.

There is a natural generalisation of these morphisms to the categorical arena.

Definition 3.2.21 A category $\mathcal{C}$ *has zero morphisms* if $\forall A, B \in \mathrm{Ob}(\mathcal{C})$ there exists a morphism $0_{A,B} : A \to B$ with the following property:

Given any two morphisms $f : A \to B$ and $g : C \to D$ the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{0_{A,C}} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ B & \xrightarrow{0_{B,D}} & D \end{array} \tag{3.39}$$

Each morphism $0_{A,B}$ is called a *zero morphism*.

Taking either f or g to be an identity yields probably the key property of a zero morphism: that composing it with any other morphism yields another zero morphism.

Proposition 3.2.22 If a category has zero morphisms then they are unique.

Example 3.2.23 FRel has zero morphisms. The zero morphism between sets X and Y is the relation which relates none of the elements of X to elements of Y. Viewed as a subset of $X \times Y$ it is the empty set.

Zero morphisms provide an ideal way of dealing with impossible processes in a theory. Suppose we have two processes which cannot be performed sequentially: for example it might be impossible to prepare a system in a certain state, represented by in the physical category $\psi : I \to A$, and then successfully perform a certain operation, $f : A \to A$, on it. If the processes of the theory are to constitute a category, then the composition $f \circ \psi$ must be well-defined. The solution is to introduce a morphism in each hom-set, representing an impossible process: then we can say that $f \circ \psi = 0_{I,A}$. Certainly, a process composed with an impossible process should be another impossible process, so it is natural to model impossible processes with zero morphisms.

Definition 3.2.24 A *zero symmetric monoidal category* (0-SMC) is a SMC with zero morphisms for which $\forall A, B, C, D \in \mathrm{Ob}(\mathcal{C})$ and $\forall f : A \to B, g : C \to D$ we have that

$$f \otimes 0_{C,D} = 0_{A \otimes C, B \otimes D} = 0_{A,B} \otimes g \tag{3.40}$$

Proposition 3.2.25 In a 0-SMC, we have a zero scalar $0_{I,I}$. Given any morphism $f : A \to B$ scalar multiplication with the zero scalar yields a zero morphism:

$$0_{I,I} \bullet f = 0_{A,B} \tag{3.41}$$

Definition 3.2.26 A dagger category *has dagger zero morphisms* if it has zero morphisms, and furthermore $\forall A, B \in \mathrm{Ob}(\mathcal{C})$ we have $0_{B,A} = 0^{\dagger}_{A,B}$.

Definition 3.2.27 A *dagger-zero symmetric monoidal category* (†-0-SMC) is a †-SMC which is a 0-SMC, and has dagger zero morphisms.

Example 3.2.28 Both **FHilb** and **FRel** are †-0-SMCs.

3.3 Basis structures and observables

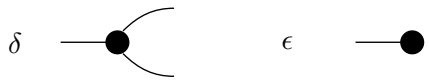
We now introduce an abstract categorical structure, the *basis structure*, which, as its name suggests, generalises the notion of an orthonormal basis. This categorical structure was first developed in a different context by Coecke and Pavlovic [13], and was subsequently used to model orthonormal bases by Coecke and Duncan [9]. The applications so far have concentrated on elucidating the interactions between different bases (in particular mutually unbiased bases) in the workings of various quantum information protocols.

We will first introduce the definition and basic properties of the basis structure in sections 3.3.1 to 3.3.4. The connection to orthonormal bases is not immediately apparent, but emerges with a small amount of work. The properties described here will be crucial to later discussions. We will subsequently proceed to develop two new applications of the basis structure. While both these applications are crucial to the remainder of this work, and both are developments of the same structure, they are quite distinct.

First, in section 3.3.5 we demonstrate that the same categorical structure used to represent orthonormal bases can also be used to provide us with an abstract counterpart to the GHZ state. The second development will be postponed to chapter 5. Here we will develop an abstract counterpart to the notion of observable. That this task should utilise basis structures is unsurprising since the key structural representative of an observable in standard Hilbert space quantum mechanics is an orthonormal basis.

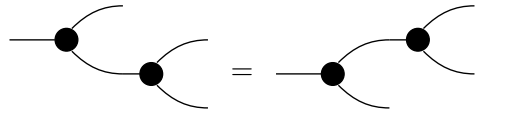
3.3.1 Definitions and examples

Definition 3.3.1 In a †-SMC $\mathcal{C}$, a *basis structure* on an object A is a triple $\Delta = \{A, \delta : A \to A \otimes A, \epsilon : A \to I\}$, where the morphisms δ and ϵ, represented graphically as:

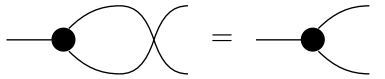


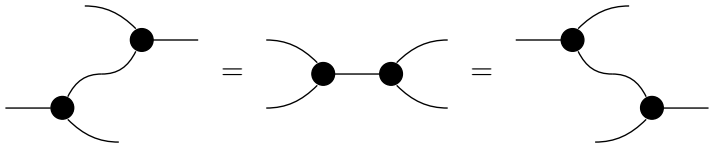
(3.42)

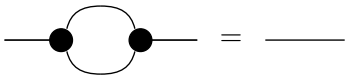
satisfy the following conditions, here given graphically:


(Coassociativity) (3.43)

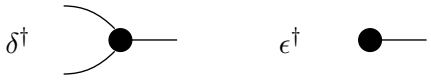

(Counit) (3.44)


(Cocommutativity) (3.45)


(Frobenius) (3.46)


(Speciality) (3.47)

Note that we are using the following graphical convention:



(3.48)

Example 3.3.2 In **FHilb**, consider a Hilbert space $\mathcal{H}$ of dimension n, with an orthonormal basis $\{|i\rangle\}_{i=1,\ldots,n}$. $\{\mathcal{H}, \delta, \epsilon\}$ constitutes a basis structure, where:

$$\delta : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H} :: |i\rangle \mapsto |i\rangle \otimes |i\rangle \qquad \epsilon : \mathcal{H} \to \mathbb{C} :: |i\rangle \mapsto 1 \tag{3.49}$$

So any orthonormal basis gives rise to a basis structure in **FHilb**. In fact the converse is also true as this important theorem shows:

Theorem 3.3.3 All basis structures in **FHilb** are of the form described in example 3.3.2.

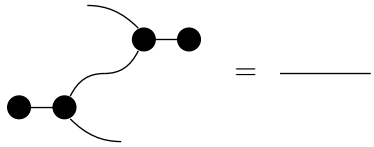
Proof: This theorem was proved by Coecke, Pavlovic and Vicary in [14]. □

These results demonstrate that basis structures in **FHilb** are in bijective correspondence with orthonormal bases, which goes some way to justifying our claim that basis structures are the abstract counterparts of observables.

3.3.2 Induced compact structure

Proposition 3.3.4 Any basis structure induces a self-dual dagger compact structure, with $A = A^*$ and $\eta_A = \delta \circ \epsilon^\dagger$.

Proof: Recalling definition 3.2.6 of a compact structure, the statement above can be re-written graphically as:



(3.50)

which is a straightforward consequence of conditions 3.46 and 3.44 (Frobenius and Counit) in definition 3.3.1. □

Example 3.3.5 Consider the **FHilb** basis structure $\Delta_Z = \{\mathbb{C}^2, \delta_Z, \epsilon_Z\}$ where:

$$\delta_Z :: \begin{cases} |0\rangle \mapsto |0\rangle \otimes |0\rangle \\ |1\rangle \mapsto |1\rangle \otimes |1\rangle \end{cases} \qquad \epsilon_Z :: \begin{cases} |0\rangle \mapsto 1 \\ |1\rangle \mapsto 1 \end{cases} \tag{3.51}$$

The induced compact structure here has:

$$\eta :: 1 \mapsto |00\rangle + |11\rangle = |\Psi_{\text{Bell}}\rangle \tag{3.52}$$

which is the compact structure which was used to introduce the notion of compact closure in section 3.2.2.

Remark 3.3.6 Note different basis structures in general give rise to different compact structures - this is illustrated by the next example. Some basis structures do give rise to the same compact structure. Such basis structures are said to have *coincident compact structures*.

Example 3.3.7 Consider the following two **FHilb** basis structures: $\Delta_X = \{\mathbb{C}^2, \delta_X, \epsilon_X\}$ and $\Delta_Y = \{\mathbb{C}^2, \delta_Y, \epsilon_Y\}$ where:

$$\delta_X :: \begin{cases} |+\rangle \mapsto |+\rangle \otimes |+\rangle \\ |-\rangle \mapsto |-\rangle \otimes |-\rangle \end{cases} \qquad \epsilon_X :: \begin{cases} |+\rangle \mapsto 1 \\ |-\rangle \mapsto 1 \end{cases} \tag{3.53}$$

$$\delta_Y :: \begin{cases} |i\rangle \mapsto |i\rangle \otimes |i\rangle \\ |-i\rangle \mapsto |-i\rangle \otimes |-i\rangle \end{cases} \qquad \epsilon_Y :: \begin{cases} |i\rangle \mapsto 1 \\ |-i\rangle \mapsto 1 \end{cases} \tag{3.54}$$

The compact structure corresponding to the first structure is:

$$\eta :: 1 \mapsto |++\rangle + |--\rangle = |00\rangle + |11\rangle \tag{3.55}$$

the same as for Δ in the previous example, while that corresponding to the second structure is:

$$\eta :: 1 \mapsto |ii\rangle + |-i-i\rangle = |00\rangle - |11\rangle \neq |00\rangle + |11\rangle \tag{3.56}$$

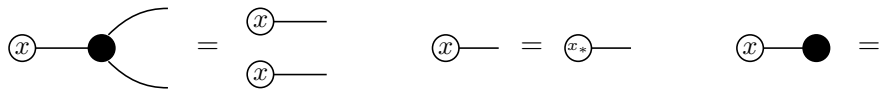
3.3.3 Eigenstates

A basis structure is supposed to be the abstract counterpart of an orthonormal basis. Can we find abstract counterparts of the basis vectors themselves? Recall that in **FHilb**, the basis vectors are copied by the δ morphism which forms part of the basis structure. We take this as our inspiration:

Definition 3.3.8 A morphism $x : I \to A$ is an *eigenstate* of a basis structure $\Delta = \{A, \delta, \epsilon\}$ iff it satisfies the following conditions:

$$\delta \circ x = x \otimes x \quad x = x_* \quad \epsilon \circ x = 1_I \tag{3.57}$$

These are depicted graphically as:



(3.58)

The first condition is simple: the eigenstates are copied by the δ operation. With the second condition we need to note that the lower star operation is relative to the compact structure which is induced by the basis structure. The third condition is a normalisation condition.

Example 3.3.9 Consider the **FHilb** basis structure of example 3.3.2. Its eigenstates are clearly $|0\rangle$ and $|1\rangle$.

We will frequently use the notation C_Δ to denote the set of eigenstates of the basis structure Δ.

3.3.4 Basis structure monoid, unbiased states and phase group

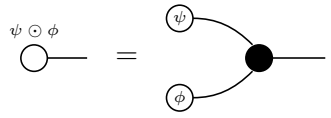
Definition 3.3.10 Given a basis structure $\Delta = \{A, \delta, \epsilon\}$ in a †-SMC $\mathcal{C}$, the *basis structure multiplication* is a map:

$$- \odot - : \mathcal{C}(I, A) \times \mathcal{C}(I, A) \to \mathcal{C}(I, A) \tag{3.59}$$

where

$$\psi \odot \phi = \delta^\dagger \circ (\psi \otimes \phi) \tag{3.60}$$

or diagrammatically:



(3.61)

Proposition 3.3.11 $(\mathcal{C}(I, A), \odot, \epsilon^\dagger)$ is a commutative monoid. We refer to this as the *basis structure monoid* corresponding to Δ.

Proof: Referring to definition 3.3.1, associativity of the basis structure multiplication follows from applying the dagger functor condition 3.43, and commutativity follows from applying the dagger functor to condition 3.45. The fact that $\epsilon^\dagger$ is a unit follows from applying the dagger functor to condition 3.44. □

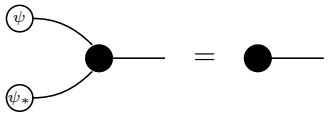
Example 3.3.12 In **FHilb** consider the basis structure on an n-dimensional Hilbert space $\mathcal{H}$, corresponding to the basis $\{|i\rangle\}_{i=1,\ldots,n}$. The basis structure multiplication on two states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ is given explicitly by:

$$|\psi \odot \phi\rangle = \sum_{i=1}^{n} \psi_i \phi_i |i\rangle \tag{3.62}$$

where ψ_i and ϕ_i are the components of $|\psi\rangle$ and $|\phi\rangle$ *in the basis corresponding to the basis structure*.

Consider a basis $\{|i\rangle\}_{i=1,\ldots,n}$ for a Hilbert space $\mathcal{H}$. Recall from section 2.1.5 that a state $|\psi\rangle$ is unbiased w.r.t this basis if, when expressed in the basis, its components $|\psi_i|^2$ are all equal[1]. Combining this fact with equation 3.62, and the fact that the lower star functor in **Hilb** corresponds to conjugation (example 3.2.20), we conclude that $|\psi \odot \psi_*\rangle = \sum_{i=1}^{n} |i\rangle$. We generalise this idea to get an abstract definition of an unbiased state:

Definition 3.3.13 Given a basis structure $\Delta = \{A, \delta, \epsilon\}$ a state $\psi : I \to A$ is *unbiased* with respect to Δ iff. $\psi \odot \psi_* = \epsilon^\dagger$. Graphically:



(3.63)

We will frequently use the notation U_Δ to denote the set of unbiased states of the basis structure Δ.

Lemma 3.3.14 $(U_\Delta, \odot, \epsilon^\dagger, (-)_*)$ is an Abelian sub-group of the basis structure monoid.

Proof: U_Δ is a subset of a commutative monoid, thus commutativity and associativity are given. The unit of the monoid is $\epsilon^\dagger$ and from condition 3.44 in definition 3.3.1 of a basis structure, we can deduce that $\epsilon^\dagger \in U_\Delta$. From equation 3.63 in definition 3.3.13, and the fact that the lower star functor is involutive we deduce that $\forall \psi \in U_\Delta$, ψ_* is also an element of U_Δ, and furthermore constitutes the group inverse for ψ. Finally we must show closure of U_Δ under $\odot$, i.e. that $(\psi \odot \phi) \odot (\psi \odot \phi)_* = \epsilon^\dagger$. We proceed as follows:

$$\begin{aligned}(\psi \odot \phi) \odot (\psi \odot \phi)_* &= (\psi \odot \phi) \odot (\psi_* \odot \phi_*) && \text{functoriality of } (-)_*, \delta_* = \delta \\ &= (\psi \odot \psi_*) \odot (\phi \odot \phi_*) && \text{coassociativity and cocommutativity} \\ &= \epsilon^\dagger \odot \epsilon^\dagger = \epsilon^\dagger\end{aligned}$$

□

Definition 3.3.15 The Abelian group of lemma 3.3.14 is termed the *phase group* of Δ.

Example 3.3.16 Consider the **FHilb** basis structure of example 3.3.2. The unbiased states are those which can be written as $|0\rangle + e^{i\phi}|1\rangle$. The phase group is isomorphic to $U(1)$.

3.3.5 GHZ states

The 3-qubit GHZ state was introduced in section 2.2.2:

$$|\Psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{3.64}$$

[1]Here we are not requiring that the state is normalised. If it is then $\forall\, i$, $|\psi_i|^2 = \frac{1}{\sqrt{n}}$, as per equation 2.5

This state can be generalised to three systems all described by state space $\mathcal{H}$, with dimension n:

$$|\Psi_{GHZ}\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |iii\rangle \tag{3.65}$$

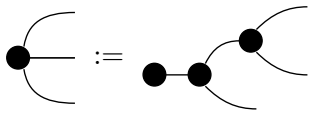
where $\{|i\rangle\}_{i=1,\ldots,n}$ is a basis for $\mathcal{H}$. Note that for each choice of basis for $\mathcal{H}$ we have a unique GHZ state. Key properties of the state include that it is symmetric under the interchange of any two of the systems, and that the application of the bra $\sum_{i=1}^{n} \langle i|$ to one system yields the Bell state $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |ii\rangle$ on the other two systems.

We now define an abstract counterpart to the GHZ state:

Definition 3.3.17 In a †-SMC, the *GHZ state* $\Psi_\Delta : I \to A \otimes A \otimes A$ corresponding to the basis structure $\Delta = \{A, \delta, \epsilon\}$ is the composition:

$$\Psi_\Delta := (\delta \otimes 1_A) \circ \delta \circ \epsilon^\dagger \tag{3.66}$$

or graphically:



(3.67)

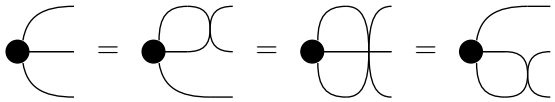
Recall that in **FHilb** each basis structure corresponds to an orthonormal basis, and in this category the definition above yields exactly the GHZ state corresponding to this basis.

Bearing in mind proposition 3.3.4 we see that the GHZ state is related via compact closed duality to the δ morphism, and furthermore that the compact structure involved is the one induced by Δ.

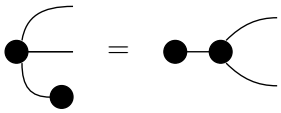
A word on notation: if the basis structure itself is labelled with a subscript, we may label the GHZ state with the same subscript to indicate the correspondence. For example the GHZ state corresponding to the basis structure Δ_1 could be labelled as Ψ_1 rather than Ψ_{Δ_1}.

In addition to coinciding with the original notion of GHZ state in **FHilb**, the abstract GHZ state has, in its own right, many of the properties of the original GHZ state:

Proposition 3.3.18 The abstract GHZ state satisfies the following equalities, expressed graphically:



(3.68)



(3.69)

Proof: Straightforward verification with graphical calculus. □

3.4 Case study: Stab, the physical category of the stabiliser theory

We conclude this section by introducing the physical category for the stabiliser theory introduced in section 2.3. First we digress briefly to discuss a category derived from **FHilb** which can more accurately claim to be the physical category for quantum mechanics. We will then define the category **Stab**, show that it is indeed the physical category for this theory, and pinpoint the concrete realisations of some of the structures introduced in earlier sections of this chapter.

3.4.1 FHilb and $\mathbf{FHilb_p}$

In the standard treatment of QM, it is well-known that states of a system correspond to the rays of the Hilbert space describing that system, rather than to individual vectors. This is because (a) Any vector representing a state must be normalised and (b) Any two such state vectors which differ only by a scalar factor with magnitude 1 (i.e. by a phase), will give identical results for the probability of any measurement outcome, and thus represent the same state. As a further consequence of this, scalar multiples of linear maps also represent essentially the same quantum operation. One might wonder why we continue to work with vectors at all, given this redundancy. Why not do all our calculations with rays, since these are the objects which genuinely represent states? Unfortunately, unlike the case of vectors, there is no well-defined algebraic structure on rays. If we dropped vectors altogether from our description, we would have no means of showing that one state is a superposition of others, since we would have lost our ability to describe relative phases, which of course *are* empirically observable.

However, in our categorical treatment of QM we make no use of the concept of superposition, or indeed of any additive structure. Thus it may make sense to quotient over scalar multiples to reduce the amount of redundant structure we are working with. There is good motivation to do this: thus far, we have claimed that **FHilb** was the physical category of pure state QM, but in the light of this discussion we see that this is not quite correct. Many different morphisms of **FHilb** will correspond to the same physical operation. The genuine physical category of QM will be derived from **FHilb** in the following fashion:

Definition 3.4.1 $\mathbf{FHilb_p}$ is the category whose objects are those of **FHilb**, and whose morphisms are the equivalence classes of **FHilb** morphisms under the following relation:

$$f \sim g \text{ iff. } \exists\, c \in \mathbb{C}\backslash\{0\}, \text{ such that } f = c.g \tag{3.70}$$

Note that in what follows, we may (slightly abusively) use a specific linear map to represent the equivalence class of which it is a member.

Proposition 3.4.2 $\mathbf{FHilb_p}$ inherits the composition, monoidal product, dagger functor and zero morphisms of **FHilb**. One can straightforwardly verify that under these operations $\mathbf{FHilb_p}$ is also a †-0-SMC. Basis structures are also inherited from **FHilb**. The equivalence

classes containing the δ and ϵ morphisms of **FHilb** themselves become the δ and ϵ morphisms of $\mathbf{FHilb}_{\mathrm{p}}$. Compact structures are similarly inherited.

Note that $\mathbf{FHilb}_{\mathrm{p}}$ has only two scalars (a zero and a 'not zero').

3.4.2 Definition of Stab

Definition 3.4.3 The category **Stab** is a sub-category of $\mathbf{FHilb}_{\mathrm{p}}$. It is defined constructively, as follows:

- The objects of **Stab** are $\mathbb{C}$, $\mathbb{C}^2$ and the n-fold tensor products $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.
- The morphisms of **Stab** are all those equivalence classes of linear maps generated by composition, tensor product and adjoint from the following generating classes:
  1. The classes containing the single qubit Clifford unitaries.
  2. The class containing the map $\delta_{\mathbf{Stab}} : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2 :: \left\{ \begin{array}{l} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{array} \right.$
  3. The class containing the map $\epsilon_{\mathbf{Stab}} : \mathbb{C}^2 \to \mathbb{C} :: \left\{ \begin{array}{l} |0\rangle \mapsto 1 \\ |1\rangle \mapsto 1 \end{array} \right.$

Stab inherits the †-0-SMC structure from $\mathbf{FHilb}_{\mathrm{p}}$. We know from example 3.3.2 that $\{\mathbb{C}^2, \delta_{\mathbf{Stab}}, \epsilon_{\mathbf{Stab}}\}$ is a basis structure, which in turn generates a compact structure.

3.4.3 Stab is the physical category of the stabiliser theory

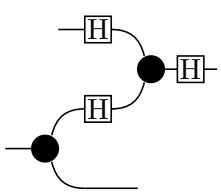
From this definition it is not at all clear that **Stab** is the physical category of the stabiliser theory. To show that it is, we proceed in several steps.

Proposition 3.4.4 The morphisms of **Stab** include all of the n-qubit Clifford operations.

Proof: The single qubit Clifford unitaries include the *Hadamard* operator which, expressed in the computational basis has the matrix form:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.71}$$

It is straightforward to verify that the following combination of the $\delta_{\mathbf{Stab}}$ morphism with the Hadamard operator is equal to the CNOT gate:



(3.72)

We recall from section 2.3.2 that any n-qubit Clifford unitary can be generated by composing the single qubit Clifford unitaries and CNOT gate. □

Proposition 3.4.5 The map $\epsilon^{\dagger}_{\mathbf{Stab}} : \mathbb{C} \to \mathbb{C}^2$ prepares the state $|+\rangle$.

Proposition 3.4.6 Given any n-qubit stabiliser state $|\Psi\rangle$ there exists some Clifford unitary U such that $|\Psi\rangle = U(|+\rangle \otimes \cdots \otimes |+\rangle)$.

Propositions 3.4.4, 3.4.5 and 3.4.6 together imply that the morphisms of **Stab** include all stabiliser states and Clifford unitaries, and can describe any Pauli measurement. Thus we conclude:

Proposition 3.4.7 The morphisms of **Stab** include all states and transformations of the stabiliser theory.

The converse is also true:

Proposition 3.4.8 The morphisms of **Stab** are all realisable in the stabiliser theory.

Proof: The generators of **Stab** are all clearly contained within the theory. $\epsilon_{\mathbf{Stab}}$ is the adjoint of the state $|+\rangle$. $\delta_{\mathbf{Stab}}$ can be obtained by composing the GHZ states with the adjoint of the Bell state. Since the stabiliser states and Clifford operations are closed under composition all morphisms in **Stab** must be states or transformations of the stabiliser theory. □

Thus we conclude that **Stab** is exactly the physical category of the stabiliser theory.

3.4.4 The basis structures of Stab

Stab is a sub-category of $\mathbf{FHilb}_{\mathrm{p}}$. Thus to understand the basis structures of **Stab** we must first understand the basis structures of $\mathbf{FHilb}_{\mathrm{p}}$.

Clearly any basis structures on $\mathbf{FHilb}_{\mathrm{p}}$ derive from those on **FHilb**. We know from theorem 3.3.3 that in **FHilb** every basis structure corresponds uniquely to an orthonormal basis. Such a basis consists of normalised vectors. Multiplying each basis vector by a phase yields a *new* basis, which corresponds to a *different* basis structure in **FHilb**. For example, it is straightforward to verify that the δ map in example 3.3.2 does *not* copy the vector $e^{i\theta}|1\rangle$, unless $\theta = 0$. In $\mathbf{FHilb}_{\mathrm{p}}$ however, these may not yield distinct basis structures:

Proposition 3.4.9 Consider two orthonormal bases $\{|j\rangle\}_{j=1,\ldots,n}$ and $\{e^{i\theta(j)}|j\rangle\}_{j=1,\ldots,n}$, on an n-dimensional space $\mathcal{H}$, where θ is a function of j. In **FHilb** these correspond to distinct basis structures. In $\mathbf{FHilb}_{\mathrm{p}}$ if $\theta(j)$ is constant for all j they correspond to the same basis structure, otherwise they correspond to distinct basis structures.

Even when we do get distinct basis structures, the states which are copied are not distinguishable within $\mathbf{FHilb}_{\mathrm{p}}$ because they differ only by scalars.

Proposition 3.4.10 Two distinct basis structures in $\mathbf{FHilb}_{\mathrm{p}}$, corresponding to the two sets of basis vectors $\{|j\rangle\}_{j=1,\ldots,n}$ and $\{e^{i\theta(j)}|j\rangle\}_{j=1,\ldots,n}$ have the same eigenstates and unbiased states.

In any †-SMC, given some basis structure $\Delta = \{A, \delta, \epsilon\}$ recall that by its definition the $\epsilon^\dagger$ map is unbiased with respect to that basis structure.

Proposition 3.4.11 Consider a basis structure, Δ in $\mathbf{FHilb}_{\mathrm{p}}$ with a given set of eigenstates C_Δ and unbiased states U_Δ. Now consider the set Σ_Δ of all other basis structures which share these eigenstates.

- All members of Σ_Δ have the same set of unbiased states, U_Δ.
- Each member of Σ_Δ has a distinct ϵ map. In each case $\epsilon^\dagger \in U_\Delta$.
- For every $u \in U_\Delta$ there is some $\Delta' = \{A, \delta', \epsilon'\} \in \Sigma_\Delta$ such that $u^\dagger = \epsilon$.

The qubit object in **Stab** has six states, the single-qubit stabiliser states. Viewed as vectors in $\mathbb{C}^2$ these constitute three bases for this space $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ and $\{|i\rangle, |-i\rangle\}$. Furthermore, given any pair which together form a basis, the other four are unbiased with respect to them. Thus, in the light of the discussion above, we deduce that the qubit object on **Stab** has twelve basis structures, each with two eigenstates, and four unbiased states.

These twelve basis structures are grouped into three families of four basis structures. Each element of the family has the same eigenstates and unbiased states. The four family members differ in which of their four unbiased states is equal to $\epsilon^\dagger$.

Proposition 3.4.12 For all twelve basis structures on the qubit object in **Stab**, the phase group is isomorphic to the four element cyclic group, Z_4.

Proof: Straightforward verification. □

Chapter 4

The category Spek

This chapter is devoted to consideration of the physical category of Spekkens's toy theory. The first three sections are very abstract: we introduce two new categories and investigate their properties without any consideration of their physical significance. We begin in section 4.1 by defining a category **Spek** in a constructive fashion analogous to the definition of **Stab**. In section 4.2 we characterise the form of the relations which constitute the morphisms of **Spek**. This is quite an involved process, and the technical details are relegated to appendix A, with section 4.2 containing quite a detailed sketch of the proof. Then in section 4.3 we define another category **MSpek**, which is closely related to **Spek**.

In section 4.4 we consider how **Spek** and **MSpek** are related to the toy theory. We note that because of the issues with the well-definedness of the toy theory raised in section 2.4.5 the question of which category is the physical category of the toy theory is not entirely clear-cut. However we do show that **MSpek** is a strong candidate for the physical category of the toy theory, in which case **Spek** is the physical category of the fragment of the theory consisting of the epistemic states of maximal knowledge. In subsequent chapters we will actually be more concerned with **Spek** than with **MSpek**, because it more closely corresponds with the category **Stab** defined in the previous chapter, and allows a clearer comparison with that category on the issue of hidden variable theories.

Since the toy theory is a quantum-like theory we would expect its physical category to exhibit some of the key features introduced in the previous chapter, and this is indeed the case. In section 4.5 we investigate some of the basis structures which arise in **Spek**.

The definition of **Spek** first appeared in a paper co-authored with Bob Coecke [10]. Much of the remainder of the chapter will appear in an extended version of this paper.

4.1 Definition and examples

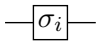
Definition 4.1.1 The category **Spek** is a subcategory of **FRel**. It is defined constructively, as follows:

- The objects of **Spek** are the single-element set I = $\{*\}$, the four element set IV :=

$\{1, 2, 3, 4\}$, and its n-fold Cartesian products IV^n.

- The morphisms of **Spek** are all those relations generated by composition, Cartesian product and relational converse from the following generating relations:

  1. All permutations $\{\sigma_i : \text{IV} \to \text{IV}\}$ of the four element set, represented diagrammatically by:

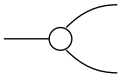
     (4.1)

     There are 24 such permutations and they form a group, S_4.

  2. A relation $\delta_{\mathbf{Spek}} : \text{IV} \to \text{IV} \times \text{IV}$ defined by:

     $$1 \sim \{(1,1),(2,2)\} \qquad 2 \sim \{(1,2),(2,1)\} \qquad 3 \sim \{(3,3),(4,4)\} \qquad 4 \sim \{(3,4),(4,3)\};$$

     represented diagrammatically by:

     (4.2)

  3. a relation $\epsilon_{\mathbf{Spek}} : \text{IV} \to \text{I} :: \{1, 3\} \sim *$ represented diagrammatically by:

     (4.3)

Remark 4.1.2 **Spek** inherits both symmetric monoidal and dagger structure from **FRel**: the monoidal product is the Cartesian product, the monoidal identity object I is the singleton set, and the dagger functor is given by the relational converse. Furthermore, perhaps unsurprisingly given the notation, $\{\text{IV}, \delta_{\mathbf{Spek}}, \epsilon_{\mathbf{Spek}}\}$ is easily seen to be a basis structure. The corresponding compact structure is $\eta_{\mathbf{Spek}} : \text{I} \to \text{IV} \times \text{IV} :: \{*\} \sim \{(1,1),(2,2),(3,3),(4,4)\}$. Given all this structure, the results of the preceding chapter would suggest that **Spek** will exhibit many quantum-like features.

4.2 General form of the morphisms of Spek

Clearly there is no limit to the number of different ways in which the generators of **Spek** can be linked together. Can we get a full characterisation of the relations which result from these combinations? For example, it's not clear that **Spek** is not in fact just the full sub-category of **FRel** restricted to the objects IV^n, i.e. $\mathbf{Spek}(\text{IV}^m, \text{IV}^n) = \mathbf{FRel}(\text{IV}^m, \text{IV}^n)$. It turns out that this is not the case - the hom-sets of **Spek** are strictly smaller than the corresponding hom-sets from **FRel**, as we will shortly show.

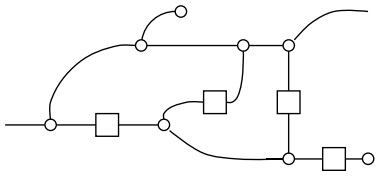
In fact our proof of the general form of **Spek** morphisms is quite lengthy, and the details are found in appendix A. In this section we give a sketch of the proof. We begin with some important pre-requisite ideas.

4.2.1 The proof is about diagrams

Definition 4.2.1 A ***Spek*** *diagram* is any valid diagram in the graphical language introduced in chapter 3 which can be formed by linking together the diagrams of the **Spek** generators, as described in definition 4.1.1.

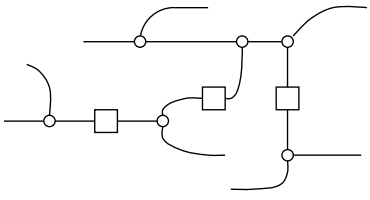
There is clearly a bijection between the possible compositions of **Spek** generators, and **Spek** diagrams. A **Spek** diagram with m inputs and n outputs represents a morphism of type $\mathrm{IV}^m \to \mathrm{IV}^n$: a relation between sets IV^m and IV^n. The number of relations between two finite sets A and B is clearly finite itself: it is the power set of $A \times B$. Thus the hom-set **FRel**(A,B) is finite. Since $\mathbf{Spek}(\mathrm{IV}^m, \mathrm{IV}^n) \subseteq \mathbf{FRel}(\mathrm{IV}^m, \mathrm{IV}^n)$ we can be sure that the hom-sets of **Spek** are finite. On the other hand, there is clearly an infinite number of **Spek** diagrams which have m inputs and n inputs - we can add more and more internal loops to the diagrams. Thus many diagrams represent the same morphism. However the morphisms of **Spek** are, by definition, all those relations resulting from arbitrary compositions of the generating relations, i.e. any relation that corresponds to one of the infinity of **Spek** diagrams. Hence any proof about the form of the morphisms in **Spek** is going to have to be a result about the relations corresponding to each possible **Spek** diagram, even though in general many diagrams correspond to a single morphism.

Note that any **Spek** diagram can be built up in several well-defined stages. Our proofs of the general form of **Spek** elements will employ induction over each of these stages. To illustrate the stages we will use this diagram:



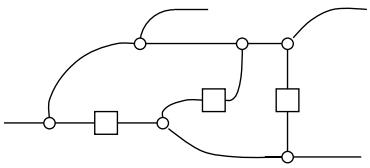
(4.4)

Firstly we can link together δ morphisms, possibly via permutations, to form a tree-like structure, without internal loops:



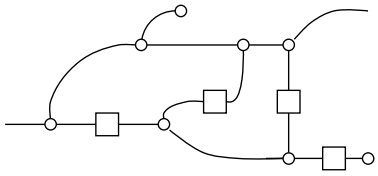
(4.5)

We'll call this the tree-level stage. Next we can link together external legs of the tree, possibly via permutations, to form loops:



(4.6)

We'll call this the loop-level stage. Finally we can add permutations and ϵ morphisms to the free ends of the diagram:



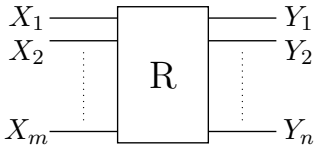
(4.7)

We'll call this the capping-level stage.

4.2.2 It's enough to show the general form of states in Spek

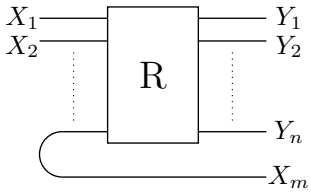
If we know the relation corresponding to one diagram in one of **Spek**'s diagram equivalence classes (recall definition 3.2.12), then it's straightforward to determine the relations corresponding to all of the other diagrams.

Lemma 4.2.2 Given a **Spek** diagram and corresponding relation:



$$R : X_1 \times X_2 \times \cdots \times X_m \to Y_1 \times Y_2 \times \cdots \times Y_n \tag{4.8}$$

then the relation corresponding to the following diagram:



(4.9)

is given by:

$$(x_1, x_2, \ldots, x_{m-1}) \sim \{(y_1, y_2, \ldots, y_n, x_m) | x_m \in X_m, (y_1, y_2, \ldots, y_n) \in R(x_1, x_2, \ldots, x_m)\} \tag{4.10}$$

where $x_i \in X_i$, $y_i \in Y_i$ and by $R(x_1, x_2, \ldots, x_m)$ we denote the subset of $Y_1 \times \cdots \times Y_n$ which is related by R to $(x_1, x_2, \ldots, x_m)$. Note that the compact structure we are using here is the canonical one induced by the basis structure appearing among the generators of **Spek** - see remark 4.1.2.

Every diagram equivalence class in **Spek** has at least one diagram of type $\mathrm{I} \to \mathrm{IV}^n$, representing a state, where we make every external line an output. Relations of this type can be viewed as subsets of the set IV^n and it will be convenient for us to concentrate on characterising these morphisms. Via lemma 4.2.2 any results on the general form of states will translate into results on the general form of all morphisms. In what follows we will therefore make no distinction between the inputs and outputs of a **Spek**-diagram: a diagram with m inputs and n outputs will simply be referred to as a $(m+n)$-legged diagram.

4.2.3 Sketch of the proof

We now present an outline of the proof of the general form of the states of **Spek**. The full proof appears in appendix A.

Phased and unphased permutations

First we need to refine the group of permutations on IV. Note from definition 4.1.1 that the generator $\delta_{\mathbf{Spek}}$ effectively partitions the elements of IV into two halves $\{1, 2\}$ and $\{3, 4\}$.

Definition 4.2.3 A *phased* permutation is an element of S_4 which maps $\{1, 2\}$ into $\{1, 2\}$ and $\{3, 4\}$ into $\{3, 4\}$. There are four such permutations: the identity, (12)(3)(4), (1)(2)(34) and (12)(34). These permutations form a subgroup of S_4, termed the *phased subgroup*. All other permutations in S_4 are termed *unphased*.

Definition 4.2.4 Spek diagrams which are generated by composition, Cartesian product and relational converse from the generators $\delta_{\mathbf{Spek}}$, $\epsilon_{\mathbf{Spek}}$, and the four *phased* permutations will be termed *phased diagrams*. All other diagrams will be termed *non-phased diagrams*.

The 'phased' terminology is chosen because the phased subgroup turns out to be isomorphic to the phase group of $\delta_{\mathbf{Spek}}$. Only a subset of the morphisms of **Spek** correspond to phased diagrams, and these will be termed *phased morphisms*. The majority of **Spek** morphisms, which correspond only to non-phased diagrams, are termed *non-phased morphisms*. The general form of a phased morphism is much simpler than the general form of a non-phased morphism. In fact our proof splits into two major stages: we first derive the general form of a phased morphism, and then use this result in our derivation of the general form of a non-phased morphism.

Phased morphisms

We begin by stating the main result on phased morphisms.

Theorem 4.2.5 (Listed as **theorem A.3.8** in appendix A)

A phased morphism in **Spek** of type $\mathrm{I} \to \mathrm{IV}^n$ is a subset of IV^n, consisting of 2^n n-tuples, divided into two classes of equal number:

- The first class consists of tuples of 1s and 2s, all of either odd or even parity.
- The second class consists of tuples of 3s and 4s, again all of either odd or even parity.

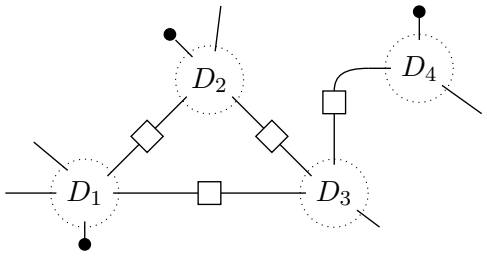
Tuples of the first class have odd parity if they have an odd number of 2s, even parity if they have an even number of 2s. Tuples of the first class have odd parity if they have an odd number of 4s, even parity if they have an even number of 4s.

The proof of this theorem proceeds in two main stages. In the first stage we define a new category, **MiniSpek** (definition A.2.1). This category is also a sub-category of **FHilb** and is defined in a very similar fashion to **Spek**. It too has one elementary object, this time a two-element set $\mathbb{II} = \{0, 1\}$, and is generated by the morphisms of a basis structure $\delta_{\mathbf{Mini}} : \mathbb{II} \to \mathbb{II} \times \mathbb{II}$ and $\epsilon_{\mathbf{Mini}} : \mathbb{II} \to \mathrm{I}$, and the four-element group of permutations on $\mathbb{II}$. The general form of **MiniSpek** morphisms is then deduced, employing induction over tree-, loop- and capping-levels (theorem A.2.3).

In the second stage we show that any phased **Spek** morphism can essentially be seen as the union of a pair of **MiniSpek** morphisms - thus by characterising the morphisms of **MiniSpek** we have done the same for the phased morphisms of **Spek**.

Non-phased morphisms

First note that a non-phased diagram can be built up in tree, loop and capping phases, analogous to our discussion in section 4.2.1, but in this case our basic units are not the three-legged $\delta_{\mathbf{Spek}}$ diagrams, but complete n-legged phased diagrams, and the permutations joining them are not members of the phase subgroup.



(4.11)

These phased sub-diagrams will be termed *zones*. If a zone has external legs we call it an *external zone*. A general **Spek** diagram consists then of phased zones linked by non-phased permutations. We now have the vocabulary to state the general form of relation corresponding to such diagrams.

Theorem 4.2.6 (Listed as **theorem A.4.2** in appendix A)

The state $\psi : \mathrm{I} \to \mathrm{IV}^n$ in **Spek** corresponding to an n-legged **Spek**-diagram with m external zones is *either*

A subset of IV^n satisfying the following properties:

1. It consists of 2^n n-tuples.
2. Each n-tuple is divided into m sub-tuples, each corresponding to an external zone in the diagram. Each sub-tuple has as many components as the corresponding zone has external legs - we will denote this number by n_i - and has a well-defined *type* (components either all 1 or 2, or all 3 or 4) and *parity* (as defined for phased relations).
3. ψ is partitioned into 2^m equally sized subsets called *blocks*. The i^{th} sub-tuple of every tuple in a block has the same type and parity. The sequence of types and parities of each sub-tuple is called the *signature* of the block. Each block has a unique signature.

4. Each block has $2^{(n-m)}$ elements: these constitute every possible combination of the sub-tuples which satisfy the parity and type requirements of the block's signature.

5. Each of the four possible combinations of parity and type appear in the i^{th} sub-tuple in one quarter of the tuples.

or it is equal to the empty set, $\emptyset$.

An example might make these definitions clearer. Consider a diagram with three external zones, the first two of which have three legs, and the third of which has two legs. The corresponding state ψ would consist of $2^8 = 256$ 8-tuples. These would be partitioned into $2^3 = 8$ blocks, each consisting of 32 tuples. The tuple (1,2,1,3,3,4,2,2) might be an element of the block with signature $(P_1 = odd, T_1 = \{1,2\}; P_2 = odd, T_2 = \{3,4\}; P_3 = even, T_3 = \{1,2\})$.

The proof of theorem 4.2.6 proceeds inductively over the tree-, loop- and capping-levels.

Tree-level diagrams

The first result here (lemma A.4.3) is to show that if the state ψ corresponding to an n-legged diagram D satisfies the five conditions of theorem 4.2.6, so too will the state ψ' corresponding to the $(n + n' - 2)$-legged diagram D' with $m + 1$ zones which is formed by connecting a new n'-legged phased zone onto D via an unphased permutation. Note that ψ' will need $2^{n+n'-2}$ tuples and 2^{m+1} blocks.

The key move in this proof is to show that every 'parent' block B of tuples in ψ begets two 'progeny' blocks B_1 and B_2 in ψ', each with $2^{n'-2}$ as many tuples as B, and further that all progeny blocks are distinct. These results ensure that ψ' has the correct number of blocks and tuples.

Having proved this result, and noting (i) that any phased diagram satisfies the five conditions in theorem 4.2.6, and (ii) that any tree-level diagram can be formed by connecting together phased diagrams via unphased permutations, we can conclude that the states corresponding to all tree-level diagrams satisfy the five conditions in theorem 4.2.6 (corollary A.4.4).

Closing chains to form loops

The loop-level is somewhat more complicated. We note that in building up a loop-level diagram from a tree-level diagram we form a loop by connecting the two ends of a *chain* of adjacent zones in the tree-level diagram.

Before proceeding further we first need to refine the group of permutations on IV further, by splitting the unphased permutations into two classes:

Definition 4.2.7 A *totally unphased* (TU) permutation is an element of S_4 which maps $\{1,2\}$ into $\{3,4\}$ and vice versa. There are four such permutations: (13)(24), (14)(23), (1324) and (1423).

Definition 4.2.8 *partially unphased* (PU) permutation is an element of S_4 which either maps 1 into $\{1,2\}$ and 2 into $\{3,4\}$ or vice versa, *and* which either maps 3 into $\{1,2\}$ and 4 into $\{3,4\}$ or vice versa. Any permutation which is not phased or totally unphased is partially unphased. There are 16 such permutations.

If any two adjacent zones in a loop are connected via a *partially unphased* permutation, then we can ensure that, when building up the diagram, this is the last connection in the loop which we make, thus closing a chain via a partially unphased permutation. Only if all the adjacent zones in a loop are joined by totally unphased permutations do we have to build up this loop by closing a chain with a totally unphased permutation. This turns out to be important: given a chain some of whose zones are connected via partially unphased permutations, closing this chain via a totally unphased, rather than partially unphased, permutation leads to considerable complications in the proof.

Closing with a partially unphased permutation

The main result here (lemma A.4.15) is to show that if the state ψ corresponding to a diagram D satisfies the five conditions of theorem 4.2.6, so too will the state ψ' corresponding to a diagram D', formed by closing a chain in D via a partially unphased permutation.

Note that D' has two less legs than D and the same number of zones. Thus we expect ψ' to have one quarter as many tuples as ψ and the same number of blocks. The key step here is to show that each parent block $B \subset \psi$ gives rise to *one* progeny block $B' \subset \psi'$ with one quarter as many tuples as B, and further that all progeny blocks are distinct. These results ensure that ψ' has the correct number of blocks and tuples.

Closing with a totally unphased permutation

This case is more complicated. First, given a diagram D and corresponding state ψ, recall that each tuple in ψ is divided into sub-tuples each corresponding to a zone in D, and that these sub-tuples have well-defined parities and types (i.e. (12) or (34)).

Definition 4.2.9 Consider a diagram D with a chain, and its corresponding state ψ. In a block $B \subset \psi$ which is *same-ended* with respect to the chain, the sub-tuples which correspond to initial and final zones of the chain have the same type. A *different-ended* block is defined analogously.

Now, we consider closing a chain in diagram D (with corresponding state ψ) to form a new diagram D' (with corresponding state ψ'), via a *totally unphased* permutation. The first step in the analysis is to show that upon doing this:

1. Blocks $B \subset \psi$ which are *same-ended* with respect to the chain give rise to *no* progeny blocks in ψ' (lemma A.4.20).

2. Blocks $B \subset \psi$ which are *different-ended* with respect to the chain give rise to *two* progeny blocks, each with one quarter as many tuples as B (lemma A.4.21).

Furthermore, the progeny blocks are not necessarily all distinct. Two distinct blocks $B, B' \subset \psi$ can be in a certain relation to one another such that the two progeny blocks of B are identical to the two progeny blocks of B' (proposition A.4.25). We term such a pair of blocks as *mirrored* with respect to the chain we are closing.

In order to derive a result for totally unphased permutations analogous to the one stated for partially unphased permutations at the beginning of the previous section we require that there are as many distinct blocks in ψ' as there are in ψ. But as it stands, some blocks (same-ended) in ψ produce no progeny blocks, some blocks (different-ended) produce two progeny blocks, and some progeny blocks may be duplicated.

Fortunately we are only interested in closing chains all of whose zones are linked by totally unphased morphisms. We go on to show that in the case of such chains:

1. The state ψ corresponding to the diagram with the chain consists entirely of pairs of blocks mirrored with respect to the chain (proposition A.4.29).
2. Either every block in ψ is same-ended with respect to the chain, or every block is different-ended with respect to the chain (proposition A.4.33).

If every block is same-ended then no blocks give rise to progeny blocks, and $\psi' = \emptyset$. If every block is different-ended then every block gives rise to two progeny blocks, but each of these is duplicated once - thus in total ψ' has as many blocks as ψ.

Thus we overcome the final obstacle to deriving the main result for totally unphased morphisms (lemma A.4.34). If we begin with a diagram D with a chain whose zones are connected only by totally unphased permutations, whose corresponding state ψ satisfies the five conditions of theorem 4.2.6, and then form a new diagram D' by closing the chain in D via a totally unphased permutation, the state ψ' corresponding to D' will also satisfy the conditions of theorem 4.2.6.

Using this result, and the one for partially unphased morphisms (lemma A.4.15), we can extend the inductive argument of corollary A.4.4 to loop-level (lemma A.4.35): the states corresponding to all loop-level diagrams *either* satisfy the five conditions of theorem 4.2.6, *or* are equal to $\emptyset$.

Capping-level diagrams

Finally we show (lemma A.4.36) that if the state ψ corresponding to an n-legged diagram D satisfies the five conditions of theorem 4.2.6, so too will the state ψ' corresponding to an $(n-1)$-legged diagram D', formed by capping off one of the external legs of D with $\epsilon_{\mathbf{Spek}}$ via an unphased permutation.

This result allows us to extend our inductive argument all the way, and conclude that all **Spek** morphisms either satisfy the five conditions of theorem 4.2.6, or are equal to $\emptyset$.

4.3 The category MSpek

We now define another category, **MSpek**:

Definition 4.3.1 **MSpek** is a sub-category of **FRel**. Its objects are the same as those of **Spek**. Its morphisms are all those relations generated by composition, Cartesian product and relational converse from the generators of **Spek**, plus the following relation:

$$\perp_{\mathbf{MSpek}} : \mathrm{I} \to \mathrm{IV} :: * \sim \{1, 2, 3, 4\} \tag{4.12}$$

Clearly any **MSpek**-diagram can be obtained from a **Spek**-diagram by capping off some external legs with $\perp_{\mathbf{MSpek}}$ diagrams.

In the appendix we derive the following result:

Proposition 4.3.2 All **MSpek** morphisms of type $\mathrm{I} \to \mathrm{IV}^n$ are subsets of IV^n containing $2^n, 2^{n+1}, \ldots, 2^{2n-1}$ or 2^{2n} n-tuples.

4.4 The physical category of the toy theory

We are interested here in the *epistemic* states and the transformations of the toy theory viewed as transformations *on the epistemic states rather than on the ontic states*. As an example of this distinction, recall (end of section 2.4.3) that the measurement disturbance corresponding to a particular outcome in the toy theory can be seen as a the non-deterministic choice of one of several permutations on IV for the ontic states, but as a well-defined relation on IV for the epistemic states.

We know that the epistemic states of the toy theory are subsets of the sets IV^n, and that the transformations on these states are relations between these sets. Thus we can see immediately that the physical category must be some sub-category of **FRel**, restricted to the objects IV^n. Furthermore we know that it cannot be the full sub-category restricted to these objects, since some subsets of IV^n clearly violate the knowledge balance principle.

We will show now that (a strong candidate for) the physical category for the toy theory in its entirety is **MSpek**, while if we restrict the toy theory to states of maximal knowledge (consistent with the knowledge balance principle), the physical category is **Spek**. We have chosen to emphasise the category **Spek** rather than **MSpek** because it is in closer correspondence with **Stab**, and a major theme of this work will be a comparison of these two categories. We could have defined some kind of '**MStab**' category, including mixed quantum states as well, and indeed there exists a construction to do this [29]. However this would unnecessarily complicate our analysis, especially since the phenomenon in which we will be particularly interested whilst comparing **Stab** and **Spek** (the existence or otherwise of local hidden variables) is exhibited perfectly well by pure states / states of maximal knowledge.

Proposition 4.4.1 The morphisms of the physical category of the toy theory are closed under composition, Cartesian product and relational converse.

Proof: There is no feature of the toy theory which would put any restrictions on which operations could be composed, so we expect the states and transformations to be closed under composition. Since the Cartesian product is used by the toy theory to represent composite systems we also expect the states and transformations to be closed under Cartesian product.

Every epistemic state corresponds to an outcome for at least one measurement (measurements correspond to asking as many questions as possible from canonical sets, epistemic states correspond to the answers). Recalling the discussion at the end of section 2.4.3, we see that given a state $\psi \subset \text{IV}^n$ the disturbance resulting from the corresponding measurement outcome can be decomposed as $\psi \circ \psi^\dagger$, where $\psi^\dagger$ is the relational converse of ψ. Thus we expect the relational converse of each state also to feature in the physical category of the theory.

The toy theory state corresponding to the subset $\Psi_{\mathbf{Spek}} = \{(1,1),(2,2),(3,3),(4,4)\} \subset \text{IV}\times\text{IV}$ (depicted in diagram 2.38) along with its relational converse are then easily seen to constitute a compact structure on IV. We thus have map-state duality, and it is straightforward then to show that if states are closed under relational converse, so is any morphism in the physical category. □

Note that this point sharpens our discussion about the consistency of the toy theory, in section 2.4.5. If the states and transformations which Spekkens has derived for up to three systems, under the operations of composition, Cartesian product and relational converse, yield states which violate the knowledge balance principle, then the theory as presented is inconsistent.

Proposition 4.4.2 All of the generating morphisms of **MSpek** are states or transformations of the toy theory, or can be derived from them by composition, Cartesian product or relational converse.

Proof: The only generator for which this is less than obvious is $\delta_{\mathbf{Spek}}$. This is formed by composing Spekkens's GHZ-like state (equation 2.39) with the relational converse of the state $\Psi_{\mathbf{Spek}}$ defined in the proof above. □

Proposition 4.4.3 All of the states and transformations derived by Spekkens in his original paper [32] are morphisms of **MSpek**. When we restrict to states of maximal knowledge all of the states and transformations are morphisms of **Spek**.

Proof: By inspection of [32]! □

Corollary 4.4.4 **MSpek** is the minimal closure under composition, Cartesian product and relational converse of the states and transformations described in [32]. **Spek** is the minimal closure under these operations of the states of [32] corresponding to maximal knowledge and the transformations which preserve them.

Proposition 4.4.5 All states $\psi : \text{I} \to \text{IV}^n$ of **MSpek** and **Spek** satisfy the knowledge balance principle on the system corresponding to IV^n viewed as one complete system. All those of **Spek** satisfy the principle maximally.

Proof: Recall that the knowledge balance principle requires that we can know the answer to at most half of a canonical question set. A system with n elementary components has 2^{2n} ontic states. A canonical set for such a system consists of $2n$ questions, each answer to a question halving the number of possibilities for the ontic state. Thus, we know the answer to m such questions ($m = 0, \ldots, n$), iff our epistemic state is a subset of IV^n with 2^{2n-m} elements. We conclude from proposition A.5.2 that all states of **MSpek** satisfy the knowledge balance principle on the system as a whole. We conclude from theorem 4.2.6 that all states of **Spek** correspond to the maximum knowledge about the system as a whole consistent with the knowledge balance principle. □

Proposition 4.4.6 All states $\psi : \mathrm{I} \to \mathrm{IV}^n$ of **MSpek** and **Spek** satisfy the knowledge balance principle on every subsystem of the system corresponding to IV^n.

Proof: Given an epistemic state $\psi \subset \mathrm{IV}^n$ of a composite system with n elementary components, the 'marginal' state on some subsystem is obtained from ψ by deleting from the tuples of ψ the components corresponding to the elementary systems which are not part of the subsystem of interest.

Suppose this epistemic state corresponds to a **Spek** or **MSpek** diagram, D. The elementary systems which are not part of the subsystem correspond to a certain collection of external legs of D, and, by lemma A.1.8, if we cap these with the **MSpek** generator $\perp_{\mathbf{MSpek}}$, the effect on the state ψ is exactly as described in the previous paragraph.

Composing a **Spek** or **MSpek** morphism with $\perp_{\mathbf{MSpek}}$ yields some morphism of **MSpek**, which by proposition 4.4.5 satisfies the knowledge balance principle. □

From corollary 4.4.4 and propositions 4.4.5 and 4.4.6 we reach two key conclusions:

- The states and transformations derived by Spekkens in [32] for systems of up to three components are all consistent with the knowledge balance principle.
- The physical category of the toy theory must, at least, contain all of the morphisms of in **MSpek**.

The second conclusion begs the question, could **MSpek** be a strict sub-category of the physical category of the toy theory i.e. could the toy theory contain operations not contained in **MSpek**? It's difficult to answer this question, since, as discussed in section 2.4.5 it is not clear what the rigourous definition of the toy theory is, or whether there is an unambiguous way to extend it beyond three systems. Certainly, **MSpek** is the physical category of a theory which coincides with Spekkens's theory up to the case of three qubits, and whose states and transformations are bound to satisfy the three rules of section 2.4.5 (the first two rules by propositions 4.4.5 and 4.4.6, and the third simply by its definition as the closure under composition of a set of generators). It is in this sense that we earlier remarked that **MSpek** is a strong candidate for the physical category of the toy theory.

4.5 The basis structures of Spek

Spek is a sub-category of **FRel** and thus inherits its basis structures from that category. The basis structures of **FRel** are of two types. Both definitions employ groups.

An Abelian group can be viewed in map theoretic terms as a triple $(X, \mu : X \times X \to X, \nu : \mathrm{I} \to X)$ where X is the underlying set, μ is the group multiplication, and ν picks out the unit element. Now consider these maps as relations, and take the converse relations of μ and ν, respectively $\delta : X \to X \times X$ and $\epsilon : X \to \mathrm{I}$. Then the triple (X, δ, ϵ) forms a basis structure in the category **FRel**:

Definition 4.5.1 A *simple* basis structure, Δ_G in **FRel** is a triple $\{N, \delta_G, \epsilon_G\}$, where N is an n-element set, and

$$\delta_G(z) = \{(z', z'') | z' * z'' = z\} \tag{4.13}$$

$$\epsilon_G(z) = \begin{cases} \{*\} & z \text{ is group identity} \\ \emptyset & z \text{ is any other } z \in N \end{cases} \tag{4.14}$$

where z, z', $z'' \in N$ and where $z' * z''$ denotes the group multiplication of G on z' and z''. We refer to G as the *underlying group* of Δ_G.

The other type of **FRel** basis structure can be formed by 'patching together' several such simple basis structures.

Definition 4.5.2 Given a set of Abelian groups $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$, each with a corresponding simple basis structure $\Delta_{G_i} = \{N_i, \delta_{G_i}, \epsilon_{G_i}\}$, a *compound* basis structure, $\Delta_{\mathcal{G}}$ in **FRel** is a triple $\{N, \delta_{\mathcal{G}}, \epsilon_{\mathcal{G}}\}$ where:

$$N = \sqcup_{i=1}^{m} N_i \tag{4.15}$$

$$\delta_{\mathcal{G}}(x) = \delta_{G_i}(x), \forall x \in N_i \tag{4.16}$$

$$\epsilon_{\mathcal{G}}(x) = \epsilon_{G_i}(x), \forall x \in N_i \tag{4.17}$$

Each of the simple basis structures will be known as a *constituent* of the compound basis structure.

The subsets N_i in definition 4.5.2 will be termed the *sectors of N with respect to $\Delta_{\mathcal{G}}$*.

Theorem 4.5.3 All basis structures in **FRel** are either simple or compound.

Proof: This key result was proved by Pavlovic in [27]. □

Evidently, the orders of the underlying groups must sum to give the cardinality of the set on which the basis structure is defined. With this in mind we see that the possibilities for the collections of underlying groups of basis structures on IV are: $\{Z_4\}, \{Z_2 \times Z_2\}, \{Z_3, Z_1\}, \{Z_2, Z_2\}, \{Z_2, Z_1, Z_1\}$ and $\{Z_1, Z_1, Z_1, Z_1\}$. Direct calculation establishes that of these, only $\{Z_2, Z_2\}$ generates a basis structure whose δ and ϵ morphisms are **Spek** morphisms.

The underlying groups are not sufficient to completely specify a basis structure in **FRel**: we also need to specify how the underlying set on which the basis structure is defined is to be partitioned into sectors, and which element of each sector is to correspond to the group identity. There are three ways of partitioning IV into two equal subsets, $\{1,2\}$ and $\{3,4\}$, $\{1,3\}$ and $\{2,4\}$, and $\{1,4\}$ and $\{2,3\}$. In each of these cases there are four possible combinations of choices for which elements should correspond to the group identity. Thus IV has twelve basis structures.

Further calculations reveal that the four basis structures corresponding to a given partition all have the same two eigenvalues: the two sectors themselves. Furthermore they all have the same four unbiased states: the other two-element subsets of IV. They differ in which of these four unbiased states is equal to $\epsilon^\dagger$.

An example is useful. The basis structure $\{\mathrm{IV}, \delta_{\mathbf{Spek}}, \epsilon_{\mathbf{Spek}}\}$, which employs the generating morphisms of **Spek** corresponds to a partition of IV into sectors of $\{1,2\}$ and $\{3,4\}$, and a choice of 1 and 3 as the elements to correspond to the group identity. This basis structure has eigenvalues $\{1,2\}$ and $\{3,4\}$, and unbiased states $\{1,3\}$, $\{2,4\}$, $\{1,4\}$ and $\{2,3\}$.

Proposition 4.5.4 For all twelve basis structures on the object IV in **Spek** the phase group is isomorphic to the four element product group $Z_2 \times Z_2$.

Proof: Direct calculation. □

Chapter 5

Hidden variables in the categorical framework

Our overall programme is to investigate which mathematical features of theories, when expressed in categorical terms, correspond to which physical features. The physical feature which we will concentrate on is the existence or otherwise of a local hidden variable theory which reproduces the results of the theory. In order to investigate this in the categorical setting, we need to translate the idea of a hidden variable theory into abstract categorical terms.

The categorical approach emphasises the structure resulting from the composition of processes: this makes it particularly suitable for the analysis of certain types of quantum-like phenomena, principally quantum protocols and information processing, and this has been the focus of most work in the field so far. In this context, the traditional preoccupations of quantum physicists e.g. the values taken by observables, and the probabilities of the outcomes of measurements, are of limited importance, and thus little effort has been made to deal with these considerations within the categorical approach. However, if we are to address the question of hidden variables within the categorical framework then we are going to have to develop the means to treat the issue of measurement of observables.

We begin in section 5.1 by briefly considering the notions of probability which might occur in physical theories, and which of these can be accommodated within the categorical framework. Next, in section 5.2, we consider the ways in which measurement in a physical theory can relate to the structure of the physical category of that theory. We need to pin this down quite precisely before we can use categorical reasoning to tell us anything about measurement. We define the notion of a physical theory *with quantum-like measurement* - in such theories measurement relates to the categorical structure in a particular way, and it will be for such theories that all of our subsequent results are valid. In such theories basis structures are very closely related to the notion of *observables*, but the two do not precisely correspond. In section 5.3 we define *observable structures*, a structure derived from basis structures, but corresponding directly with observables in the physical theory.

If we are to consider *local* hidden variables, we must have a clear idea of which objects in the physical category correspond to elementary systems, and which to composite systems, and

this point is addressed briefly in section 5.4. We then go on in section 5.5 to make the key definitions which allow us to discuss hidden variable theories in the abstract setting. Our definitions at this stage also encompass *non-local* hidden variables, and in sections 5.6 and 5.7 we go on to give an abstract account of *local* hidden variables.

This chapter builds on some preliminary ideas about defining hidden variables which first appeared in a paper co-authored with Bob Coecke and Rob Spekkens [11].

5.1 Generalised probabilistic theories

We now make a brief digression to discuss notions of probability which can arise in physical theories. Quantum mechanics is a *probabilistic* theory, in that it assigns probabilities to the different outcomes of a measurement. The notion of a probabilistic theory will be familiar to most readers, but we will re-cap for completeness. This definition can be applied to any theory for which systems have observables, which can be measured, yielding some outcome.

Definition 5.1.1 A *probabilistic* theory assigns to each measurement outcome of each observable a positive real number between 0 and 1, called a *probability*. Denoting an observable by A, and the exhaustive set of outcomes of a measurement of that observable by $\{a_i\}_{i=1,\ldots,n}$, we denote the probability assigned to outcome a_i by $p(a_i)$. The probabilities assigned, in general, depend on the state of the system, but in all cases the probabilities must satisfy the following condition for all observables:

$$\sum_{i=1}^{n} p(a_i) = 1 \tag{5.1}$$

The interpretation of probabilities is an involved subject, but some points are clear. Outcomes assigned a probability of 0 are impossible. Outcomes assigned a probability of 1 are certain. Many interpretations exist for the probabilities between 0 and 1!

We can also have a simpler type of theory which states simply whether an outcome is possible or impossible.

Definition 5.1.2 A *possibilistic* theory assigns to each measurement outcome of each observable an element of the two-element Boolean algebra $\mathbb{B}_2$, called a *possibility*. Using the same notation for observables and outcomes as before, we denote the possibility assigned to outcome a_i by $p(a_i)$. Possibilities must satisfy the following condition for all observables:

$$\bigvee_{i=1}^{n} p(a_i) = 1 \tag{5.2}$$

It is possible to have intermediate theories assigning a more general notion of likelihood to outcomes. We will not go into any detail here, but just note that our framework will be able to accommodate a wider range of theories than just probabilistic and possibilistic, so long as these theories have certain key features. For example, these *generalised probabilities*

should be ordered (at least partially) with a bottom element, representing impossibility, and a top element, representing the maximum level of likelihood (for probabilistic theories this is *certainty*, for possibilistic theories merely *possibility*). It should be possible to combine them in some commutative and associative fashion (in probabilistic theories this is addition, $+$, in possibilistic theories it is join, $\vee$), and so on. Bearing in mind the possibility of these alternative theories, we will henceforth refer to *generalised probabilistic theories*. We will use 0 to represent the bottom element, 1 to represent the top element, and $+$ to represent whatever operation the theory uses to combine generalised probabilities.

5.2 Theories with quantum-like measurement

The physical category of a theory supplies a lot of information about the theory, but it doesn't give the whole story by any means. For example, whilst we know that morphisms represent physical processes undergone by systems, the category tells us nothing about what sort of physical processes each morphism represents, or under what circumstances different morphisms will be realised. Some evolutions in the theory may be probabilistic, and, as we will shortly see, the category itself can give only limited information about the probabilities of different outcomes. The category tells us nothing about the values taken by the attributes of the system.

The categorical approach has so far largely been used to address the question of what information processing protocols are possible in a theory (e.g. [1], [9]), and almost no 'non-categorical' input is required to draw useful conclusions about this question. However, when dealing with the issues of measurements of observables and probabilities of measurement outcomes, we will need to supplement the information from the category with considerably more non-categorical input.

We will shortly define a certain type of theory, by the way in which certain features of its physical category relate to the description of measurement within the theory. In this chapter and the next we will show how the structure of the physical category can tell us a great deal about measurements, probabilities and the possibility of hidden variable interpretations *in this type of theory*. However, if measurements and probabilities in a theory relate to the morphisms of the physical category in a different way, or if they are absent entirely as concepts within the theory, then this categorical analysis will tell us nothing useful about the theory. In fact the non-cateogorical input is even more important than this: without knowledge of a few key pieces of non-categorical information we will be unable to formulate several important structures which we need for our (largely) categorical treatment of hidden variables.

Here is the key definition:

Definition 5.2.1 Consider a generalised probabilistic theory, whose physical category is a †-0-SMC. We say that this theory *has quantum-like measurement* if it exhibits the following features:

1. Every observable of a system in the theory is associated with one or more basis structures of the corresponding object A in the theory's physical category. Each basis structure corresponds to a unique observable.

2. Given an observable, and a corresponding basis structure Δ, there is a bijection between the possible outcomes of a measurement of that observable, and the eigenstates $\{x_i : I \to A\}_{i=1,\ldots,n}$ of Δ.

3. A measurement results in a disturbance to the state of a system. If $x_i : I \to A$ is the eigenstate corresponding to an outcome of the measurement on a system A then the resulting disturbance is described, in the physical category, by the morphism $x_i \circ x_i^\dagger : A \to A$.

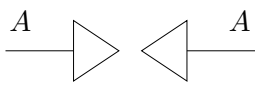
4. If the system A is prepared in a state $\psi : I \to A$ the generalised probability assigned by the theory to an outcome corresponding to eigenstate $x_i : I \to A$ is some function of the scalar $x_i^\dagger \circ \psi$. We refer to such a scalar as a *state-outcome scalar*. The function is termed the *scalar-probability function* and must be such that it maps a zero state-outcome scalar to a generalised probability of zero.

Example 5.2.2 Both the stabiliser theory and Spekkens's toy theory (with the epistemic states playing the role of the 'states' in the previous definition) have quantum-like measurement.

These points all merit some further discussion. Point (1) is somewhat puzzling in that it allows multiple basis structures to correspond to the same observable. The reason is that it's possible for two different basis structures to have the same eigenstates. We have seen examples of this in the cases of **Stab** and **Spek**. Clearly these represent the same observable within the theory. This will be dealt with in more detail in the next section.

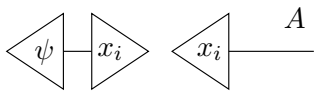
Can we give any kind of justification for the features of a theory with quantum-like measurement in physical terms? The physical significance of having the morphisms associated with measurement outcomes be the eigenstates of a basis structure is not completely clear at present. All we can say is that this correspondence does exist in all the theories so far analysed within the categorical approach.

We can do better for point (3). In QM, the measurement disturbance results in the system being prepared in a new state which depends only on the measurement outcome, not on the original state of the system. In any theory for which this is true, bearing in mind the discussion of the interpretation of morphisms in a physical category at the end of section 3.1.4, we would expect the morphism representing measurement disturbance to have the schematic form:



(5.3)

Finally, point (4), the relationship between state-outcome scalar and generalised probability. Suppose, having prepared the system in a state $\psi : I \to A$, a measurement outcome, with corresponding eigenstate $x_i : I \to A$ is impossible. Given the discussion of zero morphisms in section 3.2.3 we would expect this composition:



(5.4)

to be equal to $0_{I,A} : I \to A$. We thus expect that, given any outcome (with corresponding eigenstate x_i) which has zero probability when the system is in state ψ, the state-outcome scalar $x_i^\dagger \circ \psi = 0_{I,I}$. This makes the beginning of a connection between the state-outcome scalar and the generalised probability of an outcome - at the very least we should be able to deduce the *possibility* of an outcome from the scalar.

The question then arises as to whether the possibilities associated with a †-0-SMC with basis structures can be fine-grained to give a generalised probabilistic theory. It may be that this is possible, but not indicated in any way by the structure of the category. Equally it may be that the structure of the scalars in the category suggest a type of generalised probability and a scalar-probability function: for example the scalars in **FHilb** are $\mathbb{C}$, and the scalar probability function is $|-|^2$ yielding standard probabilities for appropriately normalised states. In general however, we don't have a clear understanding of how to derive anything other than possibilities from the state-outcome scalars of the physical category. In particular it is unclear how the scalar-probability function relates to the structure of the category, if it does at all.

In the remainder of this chapter we will attempt to develop a categorical definition of hidden variables which is general enough to encompass all generalised probabilistic theories with quantum-like measurement. This will require us to employ various 'non-categorical' data, such as the scalar-probability function. In the next chapter, we will focus on developing an abstract version of the GHZ no-go proof against hidden variables. Here the only relevant issue will be whether a measurement outcome is possible or not. This work then will require rather less 'non-categorical' input.

5.3 Observable structures

We noted in the previous section that, in general, one observable in a theory may correspond to multiple basis structures in its physical category.

Definition 5.3.1 Two basis structures $\Delta_1 = \{A, \delta_1, \epsilon_1\}$ and $\Delta_2 = \{A, \delta_2, \epsilon_2\}$ are *observably equivalent* if they have identical sets of eigenstates.

We have seen examples of observably equivalent basis structures in **Stab** (section 3.4.4) and **Spek** (section 4.5). On the object $\mathbb{C}^2$ in **Stab** there are twelve basis structures, falling into three families - the basis structures in each family are observably equivalent. A similar situation prevails in **Spek**.

Observable equivalence is clearly seen to be an equivalence relation on $\mathcal{B}_A$. The equivalence classes correspond more directly to observables than do the basis structures.

Definition 5.3.2 An *observable structure*, Ω, on an object A is an equivalence class of basis structures on A, under the relation of observable equivalence.

We conventionally denote observable structures with a capital omega, Ω, using subscripts or superscripts to distinguish between them. We denote the set of observable structures on an object A by $\mathcal{O}_A$.

Definition 5.3.3 We refer to the common set of eigenstates shared by all members of an observable structure Ω as the *values* or *outcomes* of Ω. We denote the set of values of Ω by C_Ω.

5.4 Elementary and composite objects

Another important piece of non-categorical information we need to introduce is whether an object represents an elementary indivisible system, or a composite system of potentially separable parts. Consider the case of quantum mechanics. The state space of a composite system is equal to the tensor product of the state spaces of the composite systems. Recall that the dimension of a tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is the product of the dimensions of its 'factor' spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. Thus a Hilbert space with prime dimension cannot be the tensor product of any non-trivial state spaces. However we can have a single system described by, say, a 4-dimensional state space (the spin state of a spin-3/2 particle for example), whilst the tensor product space of a pair of qubits also has dimension four, being the product of two 2-dimensional spaces. From the point of view of the category **FHilb** these are two isomorphic objects, and thus cannot be distinguished in categorical terms.

For our purposes however, whether an object represents an elementary or composite system is crucial. In fact in the case of our two key examples **Stab** and **Spek** this issue is side-stepped: in each case the category is constructed so that there is just one non-trivial object which cannot be written as the monoidal product of any other object ($\mathbb{C}^2$ and IV respectively), and it is exactly this object which is interpreted as representing an elementary indivisible system, with all other objects representing composite systems. However, more generally we will have to put the distinction between elementary and composite objects 'in by hand'.

5.5 Abstract hidden variables

Throughout the remainder of this chapter our setting will be a generalised probabilistic theory with quantum-like measurement, and its physical category $\mathcal{C}$. The generalised probabilities take their values in $\mathbb{P}$, and the scalar-probability function is denoted by $\mathcal{P} : \mathcal{C}(I, I) \to \mathbb{P}$.

Definition 5.5.1 The *outcome set* of an object A is the set $\mathcal{R}_A = \bigcup_{\Omega \in \mathcal{O}_A} C_\Omega$.

Note that $\mathcal{R}_A$ may be only a proper subset of $\mathcal{C}(I, A)$. The two will only be equal if every state of A is an eigenstate of some basis structure of A.

Definition 5.5.2 An *outcome probability function* (OPF) on an object A is a function P :

$\mathcal{R}_A \to \mathbb{P}$ such that:

$$\forall\, \Omega \in \mathcal{O}_A, \quad \sum_{x \in C_\Omega} P(x) = 1 \tag{5.5}$$

i.e. the probabilities assigned by the OPF are normalised over the outcomes of all observables.

An OPF corresponds with the intuitive notion of a state: some mathematical entity which gives us the probability of every measurement outcome. Indeed, every state in the theory (i.e. every morphism of type $I \to A$) gives rise to an OPF:

Proposition 5.5.3 A state $\psi : I \to A$ naturally gives rise to an OPF, termed the *outcome probability function of* ψ, via the prescription:

$$P_\psi : \mathcal{R}_A \to \mathbb{P} :: x \mapsto \mathcal{P}(x^\dagger \circ \psi) \tag{5.6}$$

Proof: The scalar-probability function by definition yields the probabilities for a generalised probabilistic theory, which, again by definition, are bound to satisfy the normalisation condition in equation 5.5. □

Note however that not every OPF that could be defined on A will arise from one of the states of A. Not all 'states', in the sense of probability distributions over measurement outcomes, will actually be realised in a given theory.

We now define the key notions which allow us to make sense of questions about hidden variables in the abstract categorical framework.

Definition 5.5.4 The *hidden state space* of an object A is the set $\Xi_A = \prod_{\Omega_i \in \mathcal{O}_A} C_{\Omega_i}$. The elements of Ξ_A are termed *hidden states*.

Each hidden state $h \in \Xi_A$ is a tuple of values. By h_i we denote the i^{th} component of the tuple h: this is interpreted as representing the value of observable Ω_i in this hidden state.

Definition 5.5.5 Each $h \in \Xi_A$ induces a *value function* $v_h : \mathcal{O}_A \to \mathcal{R}_A :: \Omega_i \mapsto h_i$.

Definition 5.5.6 A *hidden state distribution* (HSD) over a hidden state space Ξ is a σ-additive measure $\mu : \mathcal{B}(\Xi) \to \mathbb{P}$, such that $\mu(\Xi) = 1$.

Proposition 5.5.7 Any HSD μ gives rise to a corresponding OPF P_μ via the following prescription. If $x \in C_{\Omega_i}$:

$$P_\mu(x) = \mu(\{h \in \Xi | v_h(\Omega_i) = x\}) \tag{5.7}$$

Proof: $\forall\, \Omega_i \in \mathcal{O}_A$, $\sum_{x \in C_{\Omega_i}} P_\mu(x) = \mu(\bigcup_{x \in C_{\Omega_i}} \{h \in \Xi | v_h(\Omega_i) = x\}) = \mu(\Xi) = 1$. □

Definition 5.5.8 A state $\psi : I \to A$ has a *hidden variable interpretation* (HVI) if there exists a HSD μ on Ξ_A such that $P_\mu = P_\psi$.

So, every object in a physical category (representing a system in the corresponding theory) which has observable structures, also has a HSS. This state space is well-defined irrespective of whether the theory actually has a hidden variable interpretation. The hidden states themselves are basically all the possible combinations of outcomes for each observable structure. Physically we interpret them as telling us the value of each observable. HSDs are simply probabilistic measures on the HSS; any HSD will yield an OPF on the object. If the OPF derived from a state of the theory coincides with the OPF derived from an HSD, then that HSD provides a hidden variable interpretation for the state.

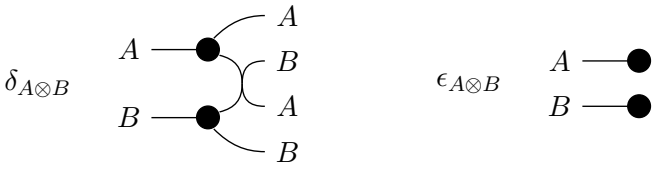
5.6 Basis and observable structures on composite objects

Definition 5.6.1 A state $\psi : I \to A_1 \otimes \cdots \otimes A_n$ is *separable* if it can be written as $\psi_1 \otimes \cdots \otimes \psi_n$ where $\psi_i : I \to A_i$. Any state which is not separable is termed *non-separable*.

Proposition 5.6.2 Two basis structures $\Delta_A = \{A, \delta_A, \epsilon_A\}$ and $\Delta_B = \{B, \delta_B, \epsilon_B\}$ induce a third basis structure, which we write as $\Delta_A \otimes \Delta_B = \{A \otimes B, \delta_{A\otimes B}, \epsilon_{A\otimes B}\}$, with:

$$\delta_{A\otimes B} = (1_A \otimes \sigma_{A,B} \otimes 1_B) \circ (\delta_A \otimes \delta_B) \qquad \epsilon_{A\otimes B} = \epsilon_A \otimes \epsilon_B \,, \tag{5.8}$$

or diagrammatically:



(5.9)

The extension to more than two basis structures is clear.

Definition 5.6.3 A basis structure on the composite object $A \otimes B$ which arises via the construction described in proposition 5.6.2 is termed a *separable basis structure*. All other basis structures on $A \otimes B$ are termed *non-separable*.

Definition 5.6.4 A physical category with basis structures satisfies the *compound observable condition* if the following two conditions are satisfied:

1. The following are equivalent:
   - The basis structures Δ_A and Δ'_A on A are observably equivalent *and* the basis structures Δ_B and Δ'_B on B are observably equivalent.
   - The basis structures $\Delta_A \otimes \Delta_B$ and $\Delta'_A \otimes \Delta'_B$ on $A \otimes B$ are observably equivalent.
2. No separable basis structure is observably equivalent to a non-separable basis structure.

Proposition 5.6.5 In a physical category satisfying the compound observable condition, two observable structures, Ω_A on A and Ω_B on B, induce a third on $A \otimes B$ which we denote as $\Omega_A \otimes \Omega_B = \{\Delta_A \otimes \Delta_B | \Delta_A \in \Omega_A, \Delta_B \in \Omega_B\}$. Such an observable structure is termed *separable*.

Proposition 5.6.6 In a physical category satisfying the compound observable condition, an observable structure on a composite object consists *either* entirely of separable basis structures, in which case it is of the form described in proposition 5.6.5, *or* entirely of non-separable basis structures. The latter are termed *non-separable* observable structures.

Example 5.6.7 Both **FHilb** and $\mathbf{FHilb}_p$ satisfy the compound observable condition.

In all our subsequent discussions we will assume that the physical category satisfies the compound observable condition.

5.7 Abstract local hidden variables

As it stands, our definitions of HSS, HSD, HVI etc. capture the idea of a hidden variable theory, but not the more specific case, in which we are interested - that of a *local* hidden variable theory. Both separable and non-separable observable structures cause problems with the interpretation of the HSS of a composite object.

Firstly we consider the separable observable structures. Suppose we have two objects A, with observable structure Ω_X and B, with observable structures Ω_Y and Ω_Z. From these we can form two further observable structures: $\Omega_X \otimes \Omega_Y$ and $\Omega_X \otimes \Omega_Z$. A hidden state $h \in \Xi_{A\otimes B}$ will have two different components h_i and h_j, one of which is a value of $\Omega_X \otimes \Omega_Y$, the other of which is a value of $\Omega_X \otimes \Omega_Z$. More formally:

$$h_i = \quad x \otimes y \in C_{\Omega_X \otimes \Omega_Y} \tag{5.10}$$

$$h_j = \quad x' \otimes z \in C_{\Omega_X \otimes \Omega_Z} \tag{5.11}$$

where $x, x' \in C_{\Omega_X}$, $y \in C_{\Omega_Y}$ and $z \in C_{\Omega_Z}$. Given the definition of a HSS (definition 5.5.4), there is no reason why x and x' should necessarily coincide. This causes problems for our interpretation of the hidden state. The natural interpretation of a separable observable structure is that it represents the simultaneous measurement of a property from each system. Furthermore, it is natural to assume that the X in the observable structures $\Omega_X \otimes \Omega_Y$ and $\Omega_X \otimes \Omega_Z$ is the same observable, but measured simultaneously with a different observable on the other system in each case. However, if we do adopt this interpretation, then hidden states such as the one above have the property that the value assigned to X on the first system depends on which observable we measure on the second system. This is exactly the kind of non-locality which was invoked in section 2.2.3 as a get-out clause for the GHZ no-go argument. We conclude that hidden states of this sort should not be allowed in a *local* hidden variable theory.

Non-separable observables are also problematic. Presumably they represent some kind of global property of the whole system, rather than individual properties of each subsystem. Nonetheless, in a local theory we would surely expect such global properties to be calculable from the local properties of each subsystem. For example, whilst the total momentum of a pair of classical particles is not a property of either particle, it is calculable from the individual momenta of the two particles. However, the HSS of a composite object contains hidden states

with identical components for separable observable structures, which differ in the components for non-separable observable structures.

These two problems can, to some extent, be avoided by tweaking the definitions of the previous section. Firstly we focus attention on separable observable structures. We denote the set of separable observable structures on a composite object A by $\mathcal{O}_A^{\text{Sep}}$.

Definition 5.7.1 The *separable outcome set* of a composite object A is the set $\mathcal{R}_A^{\text{Sep}} = \bigcup_{\Omega \in \mathcal{O}_A^{\text{Sep}}} C_\Omega$.

Definition 5.7.2 A *separable outcome probability function* (SOPF) on a composite object A is the restriction of an OPF to the separable outcome set.

As with OPFs, states naturally give rise to SOPFs:

Proposition 5.7.3 A state ψ on a composite object $A = A_1 \otimes \cdots \otimes A_n$ naturally gives rise to a SOPF, termed the *local outcome-probability function of* ψ, via the prescription:

$$P_\psi^{\text{Sep}} : \mathcal{R}_A^{\text{Sep}} \to \mathbb{P} :: (x_1 \otimes \cdots \otimes x_n) \mapsto \mathcal{P}((x_1 \otimes \cdots \otimes x_n)^\dagger \circ \psi) \tag{5.12}$$

Next we modify our hidden variable definitions from section 5.5 to make them 'local':

Definition 5.7.4 The *local hidden state space* (LHSS) of a composite object $A = A_1 \otimes \cdots \otimes A_n$ is the set $\Lambda_A = \prod_{i=1}^n \Xi_{A_i}$.

where we recall that Ξ_{A_i} denotes the hidden state space (HSS) of the object A_i.

The hidden states of an LHSS are again tuples of values. However, this time it will be convenient to index the components of the tuple with two labels: h_j^i. This represents the value of observable Ω_j on the constituent system A_i.

Definition 5.7.5 Each $h \in \Lambda_A$ induces a *value function* on each constituent object A_i:

$$v_h^i : \mathcal{O}_{A_i} \to \mathcal{R}_{A_i} :: \Omega_j \mapsto h_j^i \tag{5.13}$$

The local hidden state distribution is defined exactly analogously to the original HSD:

Definition 5.7.6 A *local hidden state distribution* (LHSD) over a local hidden state space Λ is a σ-additive measure $\mu : \mathcal{B}(\Lambda) \to \mathbb{P}$, such that $\mu(\Lambda) = 1$.

Proposition 5.7.7 Any LHSD μ gives rise to a corresponding SOPF, via the following prescription:

$$P_\mu^{\text{Sep}}(x_1 \otimes \cdots \otimes x_n) = \mu(\{h \in \Lambda | v_h^1(\Omega_{i_1}) = x_1, \ldots v_h^n(\Omega_{i_n}) = x_n\}) \tag{5.14}$$

where $\Omega_{i_j} \in \mathcal{O}_{A_j}$ and $x_j \in C_{i_j}$.

Proof: Entirely analogous to proof of proposition 5.5.7. □

Definition 5.7.8 A state $\psi : I \to A$, with $A = A_1 \otimes \cdots \otimes A_n$, has a *local hidden variable interpretation* (LHVI) if there exists a LHSD μ on Λ_A such that $P_\mu^{\text{Sep}} = P_\psi^{\text{Sep}}$.

Appearing in the hidden states of a LHSS is a unique eigenstate from each observable structure on the individual constituent objects, thus solving the first problem we faced with interpreting an HSS in terms of a local hidden variable theory. The second problem is also addressed, since hidden states of an LHSS no longer contain eigenstates for non-separable observable structures.

Chapter 6

Spek and Stab, phase group and locality

In this chapter we bring together the various strands of our story. We have translated two key examples of quantum-like theories into the categorical framework: the stabiliser theory, which is a sub-theory of standard QM, and whose physical category is **Stab**; and Spekkens's toy theory, whose physical theory is **Spek**. In section 6.1 we compare the two categories, noting that they are very similar, but identifying a key difference: the phase groups of the basis structures on the elementary objects of the categories are different, for **Stab**, Z_4, for **Spek**, $Z_2 \times Z_2$.

We go on to connect this observation with the other major strand of the story - the categorical treatment of local hidden variables. We will show that the difference in phase groups is directly related to the key physical difference between the two theories: that the toy theory has a local hidden variable interpretation, while the stabiliser theory does not. In sections 6.2 and 6.3 we explain the connection between the phase group of a basis structure Δ and the generalised probabilities of the outcomes of measurements of certain local observables on the corresponding GHZ state Ψ_Δ. In section 6.4 we show that in the case of **Stab** these generalised probabilities allow for a no-go proof ruling out a LHVI for the GHZ state. This proof is essentially the standard Mermin argument [24] introduced in section 2.2.2 recast in the language of the categorical framework. We also show that because the phase group of **Spek** is different, the generalised probabilities in this case *do not* allow for the construction of a no-go proof. Thus we trace the non-locality of the stabiliser theory to its Z_4 phase group.

In section 6.5 we generalise this result to a much wider class of phase groups. Given a basis structure with a phase group satisfying two key conditions, we can construct a generalisation of the Mermin argument. This leads to a purely group theoretic criterion for whether or not the corresponding GHZ state has a LHVI. We show that this criterion is closely related to the well-known issue of *group extensions*.

The results of section 6.1 first appeared in a paper co-authored with Bob Coecke and Rob Spekkens [11]. The results of sections 6.2-4 also essentially appeared in this paper, although they have been extensively re-worked in this chapter.

6.1 Spek and Stab compared

Compare the definitions of the categories **Stab** (definition 3.4.3) and **Spek** (definition 4.1.1). There are clear structural similarities. Both are sub-categories of a †-SMC, of the following form:

- The objects are the monoidal unit object I, an elementary object A, and n-fold monoidal products $A \otimes A \otimes \cdots \otimes A$.
- The morphisms are all those generated by composition, monoidal product and dagger functor from the following generating morphisms:
    1. Twenty-four morphisms $\sigma_i : A \to A$ combining together as the group S_4.
    2. The δ and ϵ morphisms of a basis structure $\Delta_A = \{A, \delta, \epsilon\}$ on A.

In **Spek** the morphisms are relations, in **Stab** they are linear maps, but of course from a categorical perspective these distinctions are irrelevant. The only important thing is how the morphisms combine together. Viewed in this light, the two categories start to look almost identical. They are generated by an essentially identical set of morphisms: any difference between the categories must reside in the way in which these morphisms combine. There is no difference in the way in which the σ_i morphisms combine, since in both cases we know that they form the group S_4. As elements of a basis structure, the δ and ϵ morphisms must also combine together in the same way in both cases, by definition. The only way in which the categories can differ is in the interaction between the group elements and the morphisms from the basis structure.

In fact we can identify a way in which the categories differ. We have seen already that in both categories, the elementary object has twelve basis structures, partitioned into three mutually complementary observable structures, each with four members. Each basis structure has two eigenstates and four unbiased states. In each category all these basis structures have the same phase group. But this phase group differs between the two categories: in **Stab** it is Z_4 and in **Spek** it is $Z_2 \times Z_2$.

In the stabiliser theory and the toy theory we have two theories which describe very similar systems and give very similar physical predictions for the behaviour of these systems, but with certain key differences e.g. whether or not they can be given a local hidden variable interpretation. When translated into the categorical framework, the two theories look very similar, but with certain key differences, for example the difference in phase groups. We will go on to make an explicit link between this physical difference between the theories and this mathematical difference between the physical categories.

In brief, we have already seen that there is a connection between basis structures and GHZ states (section 3.3.5). Shortly we will see that this connection extends to a link between the phase group, and the correlations between outcomes of measurements performed on the three systems in a GHZ state. We have already seen (section 2.2.2) that these correlations are a key ingredient in one of the no-go theorems ruling out hidden variable interpretations of quantum mechanics.

6.2 Forbidden triples and all-or-nothing no-go proofs

Whilst we are initially focussing on comparing **Stab** and **Spek**, we would eventually like to derive the most general possible conclusions about the links between the phase groups of basis structures, and the possibility of LHVIs. For this reason we will work in the most general setting possible, that of generalised probabilistic theories with quantum-like measurement.

Definition 6.2.1 Consider a state $\Psi : I \to A_1 \otimes \cdots \otimes A_n$ in a physical category $\mathcal{C}$. An n-tuple of values $(x_1, x_2, \ldots, x_n)$, where $x_i \in C_\Omega$, $\Omega \in \mathcal{O}_{A_i}$, is termed a *forbidden outcome n-tuple with respect to* Ψ if:

$$(x_1 \otimes x_2 \otimes \cdots \otimes x_n)^\dagger \circ \Psi = 0 \tag{6.1}$$

n-tuples which are not forbidden with respect to Ψ are *allowed* with respect to it.

The terminology is justified since, as noted in section 5.2 any generalised probabilistic theory with quantum-like measurement will assign to such a tuple of outcomes a generalised probability of zero. We now show how forbidden tuples facilitate a particular type of 'no-go' proof, ruling out a LHVI for a state.

Definition 6.2.2 An *observable n-tuple* on a composite object $A = A_1 \otimes \cdots \otimes A_n$ is a tuple of observable structures $(\Omega_1, \ldots, \Omega_n)$ where $\Omega_i \in \mathcal{O}_{A_i}$.

Lemma 6.2.3 If the value functions of a hidden state h map an observable n-tuple into an outcome n-tuple which is forbidden with respect to a state Ψ, then for a LHVI of Ψ to exist, the corresponding LHSD must assign a generalised probability of zero to h.

Proof: Recall the definition of a LHVI from section 5.7. Suppose a compound object $A = A_1 \otimes \cdots \otimes A_n$ has a LHSS Λ. A state $\Psi : I \to A$ has a *local hidden variable interpretation* (LHVI) when there exists a LHSD μ such that, for each choice of observable structures $\Omega_{i_1} \in \mathcal{O}_{A_1}, \ldots \Omega_{i_n} \in \mathcal{O}_{A_n}$, and each choice of eigenstates $x_1 \in C_{\Omega_{i_1}}, \ldots x_n \in C_{\Omega_{i_n}}$:

$$\mu(\{h \in \Lambda | v_h^1(\Omega_{i_1}) = x_1, \ldots v_h^n(\Omega_{i_n}) = x_n\}) = \mathcal{P}((x_1^\dagger \otimes \cdots \otimes x_n^\dagger) \circ \Psi) \tag{6.2}$$

If $(x_1, \ldots, x_n)$ is a forbidden tuple then the RHS of this equation must be equal to zero. Clearly then so is the LHS, from which we can conclude that all hidden states $h \in \Lambda$ for which $v_h^j(\Omega_{i_j}) = x_j$ must be assigned a generalised probability of zero. □

The key point is that knowledge of the forbidden tuples of a state of an object A allows us to deduce that certain hidden states in the LHSS of A *must* be assigned zero probability by any LHSD which aspires to be a LHVI for the state.

Definition 6.2.4 An *all-or-nothing no-go proof* against a LHVI for a state Ψ is one in which we use our knowledge of the forbidden tuples of Ψ along with lemma 6.2.3 to conclude that for a LHVI for Ψ to exist, the corresponding LHSD must assign a generalised probability of zero to *all* hidden states in the LHSS of Ψ. But by its definition a LHSD must assign a non-zero generalised probability to some states. Thus we have a contradiction, and conclude that no LHVI exists.

We will shortly see an example of exactly this type of proof.

Throughout the remainder of this chapter we will only be interested in GHZ states, and if we refer to an outcome n-tuple as forbidden, we will mean that it is forbidden with respect to whichever GHZ state is under consideration. Since the GHZ states are states on a 3-composite object, we will be referring throughout to *forbidden outcome triples*, or, for short, *forbidden triples*.

6.3 Phase group, monoid and forbidden triples

In this section we show that the phase group of a basis structure gives information on which outcome triples are allowed and forbidden with respect to its corresponding GHZ state.

6.3.1 Basis structure monoid and forbidden triples

Recall now the definition and properties of the *basis structure monoid*, from section 3.3.4. Given a basis structure $\Delta = \{A, \delta, \epsilon\}$, the corresponding monoidal product on two points $a, b : I \to A$ is defined by $a \odot b = \delta^\dagger \circ (a \otimes b)$. We will now show that this monoid catalogues the forbidden triples of the GHZ state corresponding to Δ.

Proposition 6.3.1 Given basis structure $\Delta = \{A, \delta, \epsilon\}$, and $x, x' \in C_\Delta$, we have that $(x^\dagger \circ x')^2 = x^\dagger \circ x'$, i.e. the state-outcome scalar of eigenstates of the same basis structure is an idempotent.

Proof: $(x^\dagger \circ x')^2 = (x^\dagger \otimes x^\dagger) \circ (x' \otimes x') = x^\dagger \circ \delta^\dagger \circ \delta \circ x' = x^\dagger \circ x'$ □

Proposition 6.3.2 Given $x, x' \in C_\Delta$, if $x^\dagger \circ x' = 1_I$ then $x = x'$.

Proof: First note that $(1_A \otimes x^\dagger) \circ \delta \circ x' = (1_A \otimes x^\dagger) \circ (x' \otimes x') = (x^\dagger \circ x') \bullet x' = x'$. Now since x is an eigenstate of δ, then $x_* = x$ w.r.t. the compact structure derived from δ. We then conclude that $(1_A \otimes x^\dagger) \circ \delta \circ x' = x \odot x'$, and thus that $x \odot x' = x'$. However we could argue completely symmetrically that $x \odot x' = x$. Thus $x = x'$. □

Hence the state-outcome scalar between two eigenstates of the same basis structure is an idempotent, and for two non-equal eigenstates this idempotent cannot be the identity.

Proposition 6.3.3 In the physical category of a theory with quantum-like measurement there are only two idempotent scalars, $0_{I,I}$ and 1_I.

Proof: In such a theory, probabilities are functions of the scalars of the category. The requirement that we can normalise states ensures that all scalars in this category have inverses,

with the exception of the zero scalar. Scalar multiplication is associative. Under an associative operation any idempotent with an inverse must be equal to the identity:

$$s = s \bullet 1_I = s \bullet (s \bullet s^{-1}) = (s \bullet s) \bullet s^{-1} = s \bullet s^{-1} = 1_I \tag{6.3}$$

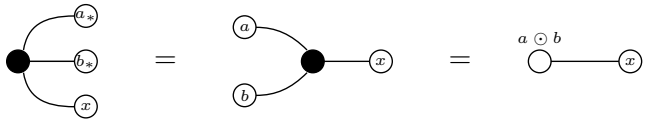
□

Proposition 6.3.4 In the physical category of a theory with quantum-like measurement, for $x, x' \in C_\Delta$, $x \neq x'$, we have that $x^\dagger \circ x' = 0_{I,I}$.

Proof: Consequence of propositions 6.3.1, 6.3.2 and 6.3.3. □

Lemma 6.3.5 Given $a, b : I \to A$, and a basis structure Δ on A with corresponding monoidal product $\odot$, suppose $\exists \Delta' \in \mathcal{B}_A$ (not necessarily equal to the original Δ) such that $a \odot b \in C_{\Delta'}$. Then $(a_*, b_*, a \odot b)$ is an allowed triple with respect to the GHZ state corresponding to Δ. Furthermore $\forall x \in C_{\Delta'}, x \neq a \odot b$, we have that (a_*, b_*, x) is a forbidden triple with respect to this GHZ state.

Proof: First note that:



(6.4)

Then if $x = a \odot b$ then the rightmost diagram equals 1_I, and $(a_*, b_*, a \odot b)$ is an allowed triple. And if $x \neq a \odot b$ the rightmost diagram equals $0_{I,I}$, and (a_*, b_*, x) is a forbidden triple. □

Hence, every pair of points a and b of A for which $a \odot b$ is an eigenstate of some basis structure has a set of associated forbidden triples. Obviously there is no overlap between these forbidden triples, since a and b are different in each case.

6.3.2 Phase groups of Stab and Spek

In this section we will retreat from the generality of the previous sections back to the specific cases of **Spek** and **Stab**. It will be the aim of subsequent sections to extend the ideas presented here to more general categories.

We have seen that in both **Spek** and **Stab** the elementary object has twelve basis structures, equally partitioned into three observable structures. We will label the three observables as Ω_X, Ω_Y and Ω_Z, in both categories. The elementary object in each case has six points, which we label as x_0, x_1, y_0, y_1, z_0 and z_1, with the labelling indicating that each observable structure has two eigenstates. The phase group is the same for all twelve basis structures, Z_4 for **Stab** and $Z_2 \times Z_2$ for **Spek**. Here are the group multiplication tables for the phase group of the basis structure with eigenstates z_0 and z_1, and $\epsilon^\dagger = x_0$, as it appears in the two

categories:

Spek

$Z_2 \times Z_2$	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_0	y_1
x_1	x_1	x_0	y_1	y_0
y_0	y_0	y_1	x_0	x_1
y_1	y_1	y_0	x_1	x_0

Stab

Z_4	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_0	y_1
x_1	x_1	x_0	y_1	y_0
y_0	y_0	y_1	x_1	x_0
y_1	y_1	y_0	x_0	x_1

(6.5)

The phase group is, by definition, a subgroup of the basis structure monoid. By lemma 6.3.5 we expect the phase group of a basis structure Δ to give us information on the forbidden triples of its corresponding GHZ state. Recall from lemma 6.3.5 that the allowed triples cannot simply be read off from the group table - the allowed triples are $(a_*, b_*, a \odot b)$. In fact, since the lower star, or conjugation operation yields the group inverse, one could equally well say that the allowed triples are $(a, b, (a \odot b)_*)$. With this in mind, we re-write the group tables above as *allowed triple tables*, by replacing each entry in the table with its group inverse:

Spek allowed triples

'$Z_2 \times Z_2$'	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_0	y_1
x_1	x_1	x_0	y_1	y_0
y_0	y_0	y_1	x_0	x_1
y_1	y_1	y_0	x_1	x_0

Stab allowed triples

'Z_4'	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_1	y_0
x_1	x_1	x_0	y_0	y_1
y_0	y_1	y_0	x_1	x_0
y_1	y_0	y_1	x_0	x_1

(6.6)

In the **Spek** ($Z_2 \times Z_2$) case, all elements of the group are self-inverse, so there is no change. In the **Stab** (Z_4) case x_0 and x_1 are self-inverse, while $(y_0)_* = y_1$.

There are two key features of these allowed triple tables which facilitate the no-go argument against HVIs: these are addressed in the next two sections.

6.3.3 Phase group gives all forbidden outcomes for certain observable triples

Each table breaks down into four two-by-two blocks. The rows of each block are labelled by the complete set of eigenstates of some observable, and the same is true for the columns.

Within each block, the entries are all eigenstates of the same observable structure. Thus, to each block we can associate a triple of observable structures:

Spek allowed triples

'$Z_2 \times Z_2$'	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_0	y_1
x_1	x_1	x_0	y_1	y_0
y_0	y_0	y_1	x_0	x_1
y_1	y_1	y_0	x_1	x_0

Stab allowed triples

'Z_4'	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_1	y_0
x_1	x_1	x_0	y_0	y_1
y_0	y_1	y_0	x_1	x_0
y_1	y_0	y_1	x_0	x_1

(6.7)

To make clear the significance of these facts, we return to the more general case of generalised probabilistic theories with quantum-like measurement. For the next few definitions and propositions we are referring to a basis structure Δ on an object A, with phase group U_Δ.

Definition 6.3.6 U_Δ is *observable-covered* if $\exists\ \{\Omega_1, \ldots \Omega_n\} \subseteq \mathcal{O}_A$ such that $U_\Delta = \sqcup_i C_{\Omega_i}$, i.e. the phase group is the disjoint union of the eigenstates of these observable structures. In this context, viewed as subsets of U_Δ the C_{Ω_i} are termed the *observable subsets* of the phase group.

For example in the cases of **Stab** and **Spek** the phase groups are both observable-covered, by the observable structures Ω_X and Ω_Y.

Definition 6.3.7 A phase group U_Δ which is observable-covered satisfies the *observable-coset condition* if one of the observable subsets is a normal sub-group of U_Δ, and the rest of the observable subsets are the cosets of this sub-group. If this condition holds we term this sub-group the *observable sub-group*, which we denote by C_0, and the cosets are termed *observable cosets*.

The phase groups on the elementary objects of **Stab** and **Spek** both satisfy the observable-coset condition. The observable sub-group is $\{x_0, x_1\}$, and there is one observable coset $\{y_0, y_1\}$.

Definition 6.3.8 The *observable quotient group* is the group $U_\Delta \backslash C_0$. Its elements are the observable cosets.

Definition 6.3.9 In an phase group U_Δ with the observable-coset property, a triple of observable structures $(\Omega_1, \Omega_2, \Omega_3)$ is said to be a *forbidden-outcome observable triple* or *FO-observable triple* if C_{Ω_1}, C_{Ω_2} and C_{Ω_3} are observable cosets and $C_{\Omega_3} = (C_{\Omega_1}.C_{\Omega_2})^{-1}$ where $-.-$ and $(-)^{-1}$ denote group multiplication and inverse with respect to the observable quotient group.

In the **Stab** and **Spek** cases there are four FO-observable triples, $(\Omega_X, \Omega_X, \Omega_X)$, $(\Omega_X, \Omega_Y, \Omega_Y)$, $(\Omega_Y, \Omega_X, \Omega_Y)$ and $(\Omega_Y, \Omega_Y, \Omega_X)$.

Proposition 6.3.10 Given an FO-observable triple $(\Omega_1, \Omega_2, \Omega_3)$, any element of $C_{\Omega_1} \times C_{\Omega_2} \times C_{\Omega_3}$ which is not of the form $(a, b, (a \odot b)_*)$ is a forbidden triple.

Proof: Any element of $C_{\Omega_1} \times C_{\Omega_2} \times C_{\Omega_3}$ which is not of the form above takes the form (a, b, x) where: (i) $x, a \odot b \in C_3$; and (ii) $x \neq a \odot b$. From lemma 6.3.5 this implies (a, b, x) is forbidden. □

6.3.4 'Parities' of allowed and forbidden triples

Within each block there is a pattern in the 'parities' of the subscript labels on the outcomes in the allowed triples. In the **Spek** case, in each block the labels sum modulo 2 to give 0. From this, and the previous point, we can deduce that for the observables XXX, XYY, YXY and YYX in **Spek**, any outcome triple with an odd number of 1s is forbidden. In the **Stab** case, the labels on the allowed triples of the XXX block sum modulo 2 to give 0, while the allowed triples of the other three blocks sum to give 1. As in the **Spek** case we can then draw conclusions about the parities of the forbidden triples for these observables.

Spek parities

'$Z_2 \times Z_2$'	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_0	y_1
x_1	x_1	x_0	y_1	y_0
y_0	y_0	y_1	x_0	x_1
y_1	y_1	y_0	x_1	x_0

0 0 0 0

Stab parities

'Z_4'	x_0	x_1	y_0	y_1
x_0	x_0	x_1	y_1	y_0
x_1	x_1	x_0	y_0	y_1
y_0	y_1	y_0	x_1	x_0
y_1	y_0	y_1	x_0	x_1

0 1 1 1

Note that the origin of these differences in parity patterns are ultimately to be found in the different phase groups in the two categories.

6.4 No-go proof from phase groups of Stab and Spek

The final stage is to try to construct an all-or-nothing no-go proof (in the sense of definition 6.2.4) for the GHZ states of **Spek** and **Stab**, using the properties of their phase groups, and what they tell us about the forbidden triples of these states.

We begin by considering a four-element phase group on an elementary object Q. We assume that the phase group is observable-covered, by two observable structures, which we will denote

Ω_X and Ω_Y. We assume further that C_X is a Z_2 sub-group of the phase group, and thus that C_Y is its coset. All of these assumptions apply equally well to the phase groups of any of the basis structures on the elementary objects of **Stab** and **Spek**.

Definition 6.4.1 The *Mermin table* for such a phase group is the following array of observable structures:

$$\begin{array}{ccc} \Omega_X & \Omega_X & \Omega_X \\ \Omega_X & \Omega_Y & \Omega_Y \\ \Omega_Y & \Omega_X & \Omega_Y \\ \Omega_Y & \Omega_Y & \Omega_X \end{array} \tag{6.8}$$

Note that the elements of each row together constitute a FO-observable triple.

Definition 6.4.2 Consider a hidden state $h \in \Lambda_{Q\otimes Q\otimes Q}$, the LHSS of $Q \otimes Q \otimes Q$. The *h-realisation* of the Mermin table is:

$$\begin{array}{ccc} v_h^1(\Omega_X) & v_h^2(\Omega_X) & v_h^3(\Omega_X) \\ v_h^1(\Omega_X) & v_h^2(\Omega_Y) & v_h^3(\Omega_Y) \\ v_h^1(\Omega_Y) & v_h^2(\Omega_X) & v_h^3(\Omega_Y) \\ v_h^1(\Omega_Y) & v_h^2(\Omega_Y) & v_h^3(\Omega_X) \end{array} \tag{6.9}$$

Note that $v_h^i(\Omega_X)$ can take two values, x_0 or x_1. A similar statement applies to $v_h^i(\Omega_Y)$. Essentially an h-realisation maps the observable triples in each row of the Mermin table into outcome triples.

Definition 6.4.3 The *parity* of a row or column of an h-realisation is the sum modulo 2 of the subscripts of the elements appearing in that row or column.

Proposition 6.4.4 In any h-realisation of any Mermin table, the parity of each of the three columns is 0.

Proof: In each column $v_h^i(\Omega_X)$ and $v_h^i(\Omega_Y)$ each appear twice. Adding either 0 to itself or 1 to itself, modulo 2, always yields 0. □

Definition 6.4.5 The *allowed parity* of a row in the Mermin table is the parity of that row in all h-realisations which assign an allowed triple to that row.

The allowed parities are well-defined in all cases, but depend on whether the phase group is Z_4 or $Z_2 \times Z_2$. We can read them off from the tables in section 6.3.4.

$$\begin{array}{lcccc} Z_4: & \Omega_X & \Omega_X & \Omega_X & 0 \\ & \Omega_X & \Omega_Y & \Omega_Y & 1 \\ & \Omega_Y & \Omega_X & \Omega_Y & 1 \\ & \Omega_Y & \Omega_Y & \Omega_X & 1 \end{array} \qquad \begin{array}{lcccc} Z_2\times Z_2: & \Omega_X & \Omega_X & \Omega_X & 0 \\ & \Omega_X & \Omega_Y & \Omega_Y & 0 \\ & \Omega_Y & \Omega_X & \Omega_Y & 0 \\ & \Omega_Y & \Omega_Y & \Omega_X & 0 \end{array} \tag{6.10}$$

Theorem 6.4.6 If U_Δ is the group Z_4, there exists no LHVI for the corresponding GHZ state.

Proof: Given any $h \in \Lambda_{Q\otimes Q\otimes Q}$, consider summing the subscripts of all elements in the h-realisation, modulo 2, to give the *table parity* for that h. We can do this by summing the parities of the three columns; from proposition 6.4.4 we conclude that for all h, the table parity is 0. Alternatively we can do it by summing the parities of the four rows. If the h-realisation maps each row into an allowed outcome triple, then from the table above we note that the table parity is 1. This is in contradiction with our previous conclusion, thus we conclude that there is no h such that the h-realisation has an allowed triple in every row. Thus every $h \in \Lambda_{Q\otimes Q\otimes Q}$ maps at least one observable triple into a forbidden outcome triple, meaning that we have an all-or-nothing no-go proof against a LHVI for Ψ_Δ. □

Corollary 6.4.7 The GHZ states on the elementary object of **Stab** do not have LHVIs. Hence we deduce that no hidden variable theory can reproduce the results of the corresponding theory, stabiliser QM.

The same argument cannot be applied to a $Z_2 \times Z_2$ phase group, because the sum of the allowed parities for the four rows is 0, not 1 as in the Z_4 case. We should expect as much, since we know that the theory corresponding to **Spek**, Spekkens's toy theory, *is* a hidden variable theory.

6.5 General relationship between phase group and non-locality

So far, we have shown that a GHZ state corresponding to a Z_4 phase group fails the Mermin table test for locality, and is inherently non-local. Conversely a GHZ state corresponding to a $Z_2 \times Z_2$ phase group does not fail the Mermin table test, and cannot be declared non-local on these grounds.

We now seek to extend this result to a general one covering a wider range of phase groups. To do this we will create a generalised analogue of the Mermin table argument applicable to other Abelian groups. We will proceed in several stages. Firstly we will show how to construct a *generalised Mermin table*, an analogue of equation 6.8. This will still have three columns, but in general many more rows, as many, in fact, as there are FO-observable triples for the phase group. Secondly we will develop a *generalised parity* to play the role of the 0 and 1 subscripts in the original argument. Thirdly we will show that in all cases the rows and columns of the generalised Mermin table have well-defined generalised parities. Once again, if the overall generalised parities of the table as calculated by the row method and column method don't match, we will have proved non-locality. Fourthly, we attempt to link passing/failing the Mermin table test to better known properties of the group.

6.5.1 Caveats

There are certain restrictions on the phase groups to which we can extend the no-go argument. The first of these is the observable-coset condition as defined in section 6.3.3. This condition is

key, since many of the definitions and results which we will soon develop are only well-defined when it holds.

The observable-coset condition is clearly a categorical property of the physical category, rather than a group theoretic property. For example it is impossible to say whether the group Z_4 has the observable coset property. However, we can say that the Z_4 phase group appearing in the elementary object basis structure in **Stab** does have the observable coset property.

The second restriction is the QSP condition. The definitions which follow in the next few sections still make sense for a phase group which does not satisfy this condition. However, our main result, theorem 6.5.16 will only apply to those which do satisfy it.

Recall that the *period* of a group element a is the smallest positive integer p such that $a^p = e$ where e is the group identity. The period is a divisor of the order of the group.

Definition 6.5.1 The *mutual period* of a group is the lowest common multiple of the periods of its elements.

Definition 6.5.2 A phase group U_Δ satisfies the *quotient-sub-period* condition, or QSP condition, if the order of the observable quotient group is a positive integer multiple of the mutual period of the observable sub-group. Put another way, in such a phase group, given any $a \in C_0$, $a^{|\mathcal{C}_Q|} = e$.

Example 6.5.3 This condition is clearly satisfied whenever the observable quotient group and observable sub-groups have equal order: this was the case in both of our previous examples, Z_4 and $Z_2 \times Z_2$. Such cases obviously only arise for phase groups of square order.

Throughout the following sections we will assume that we are dealing with a phase group U_Δ, which satisfies the observable-coset property, and corresponds to a basis structure $\Delta = \{A, \delta, \epsilon\}$. We will explicitly note when we require a phase group to satisfy the QSP condition.

6.5.2 Observable quotient group and generalised Mermin table

Recall the definition of the observable quotient group $\mathcal{C}_Q = U_\Delta / C_0$.

Throughout this section we will denote the observable sub-group by C_0, and the observable-cosets by $C_1, C_2, \ldots$ etc. The corresponding observable structures will be denoted by $\Omega_0, \Omega_1, \ldots$ etc. $C_0, C_1, \ldots$ are the elements of $\mathcal{C}_Q$. We will denote the group multiplication by $-.-$ and the inverse operation by $(-)^{-1}$.

For the remainder of these sections we will use n to denote the order of the observable quotient group i.e. $n = |\mathcal{C}_Q|$.

Definition 6.5.4 The *generalised Mermin table* of a phase group U_Δ satisfying the observable-coset condition is an array of observable structures of n^2 rows and three columns, with each row being of the form:

$$\Omega_i \quad \Omega_j \quad \Omega_k$$

where $i, j = 0, \ldots, n-1$ and the corresponding observable-cosets satisfy $C_k = (C_i.C_j)^{-1}$, i.e. each row contains the elements of a FO-observable triple. Clearly the rows are indexed by i and j so we will refer, for example to the $(i,j)^{\text{th}}$-row.

This generalises the Mermin table employed in our no-go proof for **Stab**.

6.5.3 Observable sub-group and generalised parities

We will denote the elements of the observable sub-group by $C_0 = \{a_0, \ldots, a_{m-1}\}$ where a_0 denotes the group identity element. Throughout the remainder of these sections we will use m to denote the order of the observable sub-group.

Definition 6.5.5 A *labelling of observable coset elements* is a function:

$$\mathcal{L} : \mathcal{C}_Q \backslash \{C_0\} \to U_\Delta :: C_i \mapsto c^i \tag{6.11}$$

such that $c^i \in C_i$, i.e. it consists of selecting a representative element from each observable coset. Each different set of choices yields a different labelling - thus there are m^{n-1} labellings.

Clearly, having chosen a labelling of observable coset elements we can write the observable coset C_i as $\{c^i \odot a_0, \ldots, c^i \odot a_{m-1}\}$.

Definition 6.5.6 Relative to a given labelling of observable coset elements, the *label* of an element $c^i \odot a_j$ is the observable sub-group element a_j. The label of an element of the observable sub-group is simply the element itself.

These labels will generalise the 0 and 1 subscripts which appeared in the **Spek** and **Stab** cases. In the next definitions, recall definition 5.7.4 of Λ_A, the local hidden state space of an object A.

Definition 6.5.7 Given a hidden state $h \in \Lambda_{A \otimes A \otimes A}$, the *h-realisation* of the generalised Mermin table of U_Δ is obtained via the following procedure. Beginning with the generalised Mermin table, with three columns, and rows of the form:

$$\Omega_i \quad \Omega_j \quad \Omega_k$$

take the value function of each observable structure:

$$v_h^1(\Omega_i) \quad v_h^2(\Omega_j) \quad v_h^3(\Omega_k)$$

Choosing a specific labelling $\mathcal{L}$, we can write this row as:

$$c^i \odot a_p \quad c^j \odot a_q \quad c^k \odot a_r$$

Remark 6.5.8 An h-realisation of a generalised Mermin table can more succinctly be described as a re-writing of the original table where every appearance of Ω_i in a given column is replaced by *the same element of* C_i, which we write as $c^i \odot a_{i'}$. The label $a_{i'}$ will be different in each column, and will depend on h.

Definition 6.5.9 The *generalised parity*, with respect to a labelling $\mathcal{L}$, of a row or column in an *h-realisation* of a generalised Mermin table is the product of all the labels of the elements appearing in that row or column. Thus, the generalised parity is an element of the observable sub-group.

For example, the generalised parity of the final example row in definition 6.5.7 is $a_p \odot a_q \odot a_r$.

6.5.4 An all-or-nothing no-go proof

Lemma 6.5.10 Consider a phase group U_Δ which satisfies both the observable-coset and QSP conditions. Given any labelling $\mathcal{L}$, *all* h-realisations of the generalised Mermin table of U_Δ will have, for all three columns, a generalised parity equal to the identity.

Proof: From the definition of a generalised Mermin table (definition 6.5.4), each of the n observable structures $\{\Omega_i\}_{i=0,\ldots,n-1}$ (corresponding to the observable sub-group C_0 and observable cosets $\{C_i\}_{i=1,\ldots,n-1}$) appear in the first and second columns of the table n times. Simple group theory tells us that $\forall\, C_i, C_k \in \mathcal{C}_Q$ there exists a unique $C_j \in \mathcal{C}_Q$ such that

$$(C_i.C_j)^{-1} = C_k \tag{6.12}$$

So, in the third column, Ω_k appears in the same row as Ω_i, for each $i = 0, \ldots, n-1$, exactly once. Thus we conclude that each of the n observable structures $\{\Omega_i\}_{i=0,\ldots,n-1}$ appear n times in the third column of the table as well.

Now focus on a particular column, for definiteness the first. The argument will apply equally to the second and third columns. From the argument above, and noting remark 6.5.8, we see, in the first column of any h-realisation of the table, there are n occurrences of some element $c^i \odot a_{i'}$ for each $i = 0, \ldots n-1$ (there is no need for the different i' to be distinct). The generalised parity of the first column of this h-realisation will be $(\bigodot_{i=0}^{n} a_{i'})^n$. Now, $\bigodot_{i'=0}^{n} a_{i'}$ is some element of C_0. Furthermore n is some integer multiple of the mutual period of C_0. Therefore $(\bigodot_{i=0}^{n} a_{i'})^n = a_0$. □

Lemma 6.5.11 Consider a phase group U_Δ which satisfies the observable-coset property. Given any labelling $\mathcal{L}$, all h-realisations which map the observable triple in the top row of the generalised Mermin table into an *allowed* outcome triple have a generalised parity for this row equal to the identity.

Proof: The top row of a generalised Mermin table is:

$$\Omega_0 \quad \Omega_0 \quad \Omega_0$$

From proposition 6.3.10 we know that all allowed outcome triples for this triple of observables are of the form $(a_i, a_j, (a_i \odot a_j)_*)$. Recall that the lower star operation gives the phase group inverse, by definition. In any h-realisation with such an outcome triple as its top row:

$$a_i \quad a_j \quad (a_i \odot a_j)_*$$

the generalised parity of the first row is clearly a_0, the identity element. □

Lemma 6.5.12 Consider a phase group U_Δ which satisfies the observable-coset property. Given any labelling $\mathcal{L}$, all h-realisations which map the observable triple in a given row of the generalised Mermin table into an *allowed* outcome triple have the same generalised parity for this row. This value of this parity will, in general, depend on $\mathcal{L}$.

Proof: Consider a general row of the generalised Mermin table:

$$\Omega_i \quad \Omega_j \quad \Omega_k$$

Recall that the value of k is determined by the observable quotient group via $C_k = (C_i.C_j)^{-1}$. Again, from proposition 6.3.10, we know that all allowed outcome triples for this triple of observables are of the form $(c^i \odot a_p, c^j \odot a_q, ((c^i \odot a_p) \odot (c^j \odot a_q))_*)$ where we have chosen a specific labelling. Note that the final outcome in the triple can be re-written:

$$((c^i \odot a_p) \odot (c^j \odot a_q))_* = (c^i \odot c^j)_* \odot (a_p \odot a_q)_* = d^k \odot (a_p \odot a_q)_* \tag{6.13}$$

where $d^k = (c^i \odot c^j)_* \in C_k$ but in general $d^k \neq c^k$, i.e. d^k is not the representative element of C_k picked out by the labelling function. This last point is important because it implies that if this outcome triple is a row in an h-realisation:

$$c^i \odot a_p \quad c^j \odot a_q \quad d^k \odot (a_p \odot a_q)_*$$

the $(a_p \odot a_q)_*$ appearing in the third column is *not* the label of that element, and hence is not what we need to use to calculate the generalised parity of this row. However, since $d^k \in C_k$ we know that there exists $a(i,j) \in C_0$ such that $d^k = c^k \odot a(i,j)$. We can then re-write the row above as:

$$c^i \odot a_p \quad c^j \odot a_q \quad c^k \odot (a(i,j) \odot (a_p \odot a_q)_*)$$

Clearly now $a(i,j) \odot (a_p \odot a_q)_*$ *is* the label for the element in the third column. We can use it to calculate the generalised parity for this row, which clearly equals $a(i,j)$. □

Definition 6.5.13 With respect to a labelling $\mathcal{L}$, the *allowed parity* for the $(i,j)^{\text{th}}$ row of a generalised Mermin table is $a(i,j) \in C_0$, defined by:

$$a(i,j) = (c^i \odot c^j \odot c^k)_* \tag{6.14}$$

where $C_k = (C_i.C_j)^{-1}$ and $c^i = \mathcal{L}(C_i) \ldots$ etc. Taking into account lemma 6.5.11 we define $a(0,0) = a_0$.

Corollary 6.5.14 Any $h \in \Lambda_A$ whose h-realisation has a generalised parity for the $(i,j)^{\text{th}}$ row which is not equal to the allowed parity $a(i,j)$, maps the observable triple in the $(i,j)^{\text{th}}$ row of the generalised Mermin table into a forbidden outcome triple. Consequently, for a LHVI to exist for the GHZ state, the corresponding LHSD must assign h a generalised probability of zero.

Proposition 6.5.15 For a phase group satisfying the observable-coset and QSP conditions the product of the allowed parities of all rows $\bigodot_{i,j=0}^{n} a(i,j)$ is independent of the labelling. We term this product the *Mermin parameter* of the phase group.

Proof: Consider a re-labelling which changes the representative element of just one of the cosets. For the coset C_m, instead of c^m we choose d^m. Note that $\exists\ a^* \in C_0$ such that $d^m = c^m \odot a^*$. Note that in all labellings $c^0 = a_0$, so we can assume that $m \neq 0$. With respect to this new labelling we get a new set of allowed parities for the rows of the Mermin table, $a'(i,j)$. We need to determine how they relate to the previous allowed parities $a(i,j)$, which were defined by the relation $c^i \odot c^j = c^k \odot a(i,j)$. There are several distinct situations to consider.

- $i,j,k \neq m$: We simply have $a'(i,j) = a(i,j)$.
- $i = m,\ j = 0$ or $i = 0,\ j = m$: $a(i,0)$ and $a(0,j)$ both equal a_0 in all labellings, so again we have $a'(i,j) = a(i,j)$. There are two such cases.
- $i = m,\ j \neq 0, m$ or $i \neq 0, m,\ j = m$: In the first instance we have $d^m \odot c^j = c^k \odot a'(m,j)$, in the second we have $c^i \odot d^m = c^k \odot a'(i,m)$, from which we conclude that in either instance $a'(i,j) = a^* \odot a(i,j)$. There are $2n-4$ such cases.
- $i = j = m$: Here we have $a'(i,j) = (a^*)^2 \odot a(i,j)$. There is one such case.
- $k = m$: Here we have $c^i \odot c^j = d^m \odot a'(i,j)$, and can thus conclude that $a'(i,j) = (a^*)^{-1} \odot a(i,j)$. There are n such cases, however two of them coincide with the second situation in this list. There is no overlap with the other situations in the list.

Overall then, we conclude that:

$$\bigodot_{i,j=0}^{n} a'(i,j) = (a^*)^{2n-2} \odot (a^*)^{-(n-2)} \odot [\bigodot_{i,j=0}^{n} a(i,j)] = (a^*)^n \odot [\bigodot_{i,j=0}^{n} a(i,j)] \tag{6.15}$$

If the QSP condition holds then $(a^*)^n = a_0$ and we have $\bigodot_{i,j=0}^{n} a'(i,j) = \bigodot_{i,j=0}^{n} a(i,j)$. Since we can move between any two labellings via a sequence where we only change the representative element of one coset, we have shown that the Mermin parameter is independent of labelling. □

Theorem 6.5.16 Given a phase group U_Δ which satisfies the observable-coset and QSP conditions, for which the Mermin parameter does not equal a_0, the corresponding GHZ state Ψ_Δ does not have a LHVI.

Proof: We will define the *table parity* of an h-realisation of a generalised Mermin table as the product of the labels of all elements appearing in the h-realisation. Clearly the table parity can be calculated either by taking the product of the generalised parities of all three columns, or by taking the product of the generalised parities of all n^2 rows. Using the column method, from lemma 6.5.10, any h-realisation must have a table parity of a_0. Using the row method, from corollary 6.5.14, any h-realisation in which every row is an allowed triple must have a table parity equal to the Mermin parameter. If the Mermin parameter is not equal to a_0, then there does not exist an h-realisation in which every row is an allowed triple i.e. every h-realisation has at least one row which is a forbidden triple for the corresponding observable triple in the generalised Mermin table. From lemma 6.2.3 we then conclude that any LHSD which was an LHVI for the GHZ state would have to assign a probability of zero to all hidden states h. But by its definition a LHSD must assign a non-zero probability to some states. Thus we have a contradiction, and conclude that no LHVI exists. □

6.5.5 Connection to group extensions

In group theory the *group extension problem* is the following: given an Abelian group G_1 and some other group G_2, find all groups G with a normal sub-group isomorphic to G_1, such that $G/G_1 \cong G_2$. We will concentrate on the special case where all three groups are Abelian.

Let us suggestively denote the elements of G_1 by $\{a_0, \ldots, a_{m-1}\}$ with a_0 the identity, and those of $G/G_1 (\cong G_2)$ by $\{C_0, \ldots, C_{n-1}\}$ with C_0 the identity. Now choose a representative element c^i from each C_i. Clearly now the elements of G are $\{c^i.a_j\}_{i=0,\ldots,n-1;j=0,\ldots,m-1}$. To fully specify G, it remains to determine the product of two arbitrary elements $(c^i.a_p).(c^j.a_q)$. Note first that:

$$(c^i.a_p).(c^j.a_q) = (c^i.c^j).(a_p.a_q) \tag{6.16}$$

Now $(a_p.a_q)$ is fully specified by G_1. It remains to determine $(c^i.c^j)$. We know that $(c^i.c^j) \in C_k = C_i.C_j$ where k is determined by G_2. Whilst, in general, $(c^i.c^j) \neq c^k$, we do know that $\exists\ \tilde{a}(i,j) \in C_0$ such that $(c^i.c^j) = c^k.\tilde{a}(i,j)$, so that we can write the product of two arbitrary elements in G as:

$$(c^i.a_p).(c^j.a_q) = c^k.\tilde{a}(i,j).(a_p.a_q) \tag{6.17}$$

Clearly the choices for $\tilde{a}(i,j)$ constitute the only degrees of freedom not pre-determined by G_1 or G_2, and thus different choices for these parameters will give us the different possible group extensions G.

The two sets of parameters $\tilde{a}(i,j)$ (which determine which group extension is realised) and $a(i,j)$ (which determine locality properties) are not identical, but are closely related.

Lemma 6.5.17 *In a phase group satisfying the observable-coset and QSP conditions, the product of the group extension parameters $\tilde{a}(i,j)$ is equal to the inverse of the Mermin parameter.*

Proof: Let us assume that we have $C_i.C_j = C_k$ and $(C_k)^{-1} = C_l$. Then the defining property of the $a(i,j)$ is $(c^i.c^j)_* = c^l.a(i,j)$ whilst that of the $\tilde{a}(i,j)$ is $c^i.c^j = c^k.\tilde{a}(i,j)$.

First note that $(c^k)_* = d^l$, with $e^l \in C_l$. Now define a new parameter $a(k) \in C_0$, such that $d^l = c^l.a(k)$, so that we have $(c^k)_* = c^l.a(k)$. From $(c^i.c^j)_* = c^k.a(i,j)$ we deduce $c^i.c^j = (c^k.a(i,j))_* = c^k_*.(a(i,j))_* = c^l.a(k).(a(i,j))_*$. We thus conclude that $\tilde{a}(i,j) = a(k).(a(i,j))_*$.

The product of the group extension parameters is $\prod_{i,j=0}^n \tilde{a}(i,j) = \prod_{i,j=0}^n (a(k).(a(i,j))_*) = (\prod_{i,j=0}^n a(k)).M_*$, where M denotes the Mermin parameter. Now note that there will be precisely n combinations of i,j for which $C_i.C_j = C_k$. Thus for each value of k, $a(k)$ will appear in the product n times. From the QSP condition we know that $a(k)^n = a_0$, thus we can conclude that $\prod_{i,j=0}^n a(k) = a_0$ and $\prod_{i,j=0}^n \tilde{a}(i,j) = M_*$. □

The most straightforward example of a group extension for G_1 and G_2 is the *direct product* $G_1 \times G_2$. In fact we can immediately show a direct product phase group won't exhibit Mermin-style non-locality:

Lemma 6.5.18 *Given a phase group satisfying the observable-coset and QSP conditions, which can be written as $G_1 \times G_2$ where G_1 is the observable subgroup, the Mermin parameter is equal to the identity element.*

Proof: The elements of $G_1 \times G_2$ can be written as (a_i, C_j). The elements of the form (a_i, C_0) form the subgroup isomorphic to G_1. Elements of the form (a_i, C_j), for constant j form a coset to this subgroup. Now recall our earlier discussion of *labellings* of the elements of cosets. Suppose we pick a particular labelling for $G_1 \times G_2$ such that $c^i = (a_0, C_i)$ for all cosets C_i. In this case we get $c^i.c^j = (a_0, C_i).(a_0, C_j) = (a_0, C_k) = c^k$, for all i,j. Recall that the *allowed parities* $a(i,j)$ are defined by $c^i.c^j = c^k.a(i,j)$. From this we conclude that in this labelling, $a(i,j) = a_0$ for all i,j, and thus that the Mermin parameter $M = \bigodot_{i,j=1}^n a(i,j)$ is also equal to a_0, for all labellings. □

The phase group of **Spek** is an example of this sort of situation. Note that the converse of this theorem is *not* true: a Z_9 phase group with Z_3 observable subgroup provides a counter-example.

Chapter 7

Conclusions and further work

Let us review the principal results of this work. We have introduced a mathematical framework, based on the categorical approach to quantum mechanics of Abramsky and Coecke, within which we can compare and contrast quantum-like theories which might initially have been formulated in terms of quite distinct mathematical structures. We have demonstrated the use of this framework, by expressing in it a well-known quantum-like theory, Spekkens's toy bit theory. We have shown that, when expressed in the categorical framework, the toy theory exhibits many of the same categorical structures as does quantum theory, and that it is precisely these structures which endow both these theories with certain 'typically quantum' features. In the process of re-expressing the toy theory within the categorical framework we have, as a by-product, demonstrated its internal consistency.

We have developed an entirely abstract treatment of hidden variables. This allows us to frame the question of whether or not a theory can be interpreted in terms of hidden variables, in any †-0-SMC with basis structures. This treatment provides us with all the tools we need for our subsequent analysis of all-or-nothing no-go theorems, and is flexible enough to accommodate a wider range of notions of probability, which should be useful in future work. Along the way we have developed a better understanding of how 'non-categorical' information should be employed alongside the structure of the physical category to draw useful conclusions about measurement outcomes in a theory.

We have demonstrated that the impossibility of interpreting the stabiliser theory in terms of hidden variables stems directly from the fact that the GHZ states on the elementary object of **Stab** derive from a basis structure with a Z_4 phase group. Such a basis structure effectively endows a physical category with 'non-locality'. We also showed why this argument does not work with a basis structure with a $Z_2 \times Z_2$ basis structure [11]. We have extended this result and given a group theoretic criterion which picks out a class of Abelian groups which, as phase groups of basis structures, endow a physical category with non-locality.

Many avenues of further research are suggested by this work. There exists a generalisation of the stabiliser states and Clifford operations beyond qubits, to d-level quantum systems. It should be possible to deduce the properties of the physical categories of these theories, which we could denote by $\mathbf{Stab}_d$, although whether they can be defined in the same way as **Stab**, as the closure of a small set of generators, is an open question. It would be interesting to see

what kinds of phase groups arise, and what this implies about the locality or otherwise of these theories.

Rob Spekkens has recently proposed a variation of the toy theory, which models *trits* rather than bits [33] i.e. the individual systems have observables with three possible outcomes rather than two. This theory is more clearly defined than the original version of the toy theory, employing symplectic structure on phase space. He has also recently returned to the original toy bit theory, and re-worked it in these terms. An obvious question is whether we can formulate the physical category of the trit theory (tentatively called $\mathbf{Spek}_3$), and whether it would be at all analogous to **Spek**. As yet Spekkens has no theories for higher level systems, but might it be possible to extend the definition of $\mathbf{Spek}_3$ to $\mathbf{Spek}_d$? How would these categories relate to $\mathbf{Stab}_d$? In fact we would expect that $\mathbf{Spek}_3 = \mathbf{Stab}_3$ since Spekkens has shown that his toy trit theory is equivalent to the qutrit stabiliser theory, in clear contrast to the bit/qubit case. How would this pattern continue as d increased beyond 3?

Much of our treatment of observables, measurements and outcome probabilities in chapter 5 is quite ad hoc, and would benefit from a more rigourous foundation. For example, the justification for associating the outcomes of measurements with the eigenstates of basis structures is, at present, quite flimsy: essentially we have adopted this rule simply because it works both for standard QM and for Spekkens's toy theory. We might hope to find a more convincing argument, beginning with reasonable physical assumptions, which would lead us to make the identification between observables and basis structures, and measurement outcomes and eigenstates. In a similar vein, would it be possible to give a general argument, on physical grounds, for how the generalised probabilities of measurement outcomes in a theory are related to the state-outcome scalars of the physical category, i.e. in the language of chapter 5, to deduce the form of the scalar-probability function?

We are able to describe locality and non-locality within our framework, but we currently have no treatment of *contextuality*. Suppose we have a system with three observables A, B and C, and further that A can be measured simultaneously with *either* B *or* C, but B and C cannot be simultaneously be measured. A hidden variable theory is *contextual* if it predicts that the outcome of measurement of A depends on which of B or C is measured simultaneously with A. Non-local theories are a special case of contextual theories: in this case A is an observable of one sub-system, and B and C are observables of another, spatially separated subsystem. Just as non-locality can be used as a 'get-out clause' from the GHZ no-go theorem, other no-go theorems (for example the Kochen-Specker theorem), which employ a single system, can be escaped by allowing a more general form of contextuality. It is commonly felt that contextuality, like non-locality, is a non-intuitive and undesirable feature for a hidden variable theory to possess. However, our definitions of local hidden state space (LHSS), local hidden state distribution (LHSD) and local hidden variable interpretation (LHVI) still allow for contextuality of observables on the individual subsystems. An obvious line of inquiry is to see how we might distinguish between contextual and non-contextual hidden variables within the categorical framework.

Our treatment of no-go theorems in chapter 6 suggests many avenues of further research. The most immediate goal is to fully elucidate the connection between the Mermin parameter of a phase group and the subject of group extensions. Beyond this there are many obvious open

questions.

If we can construct a no-go theorem ruling out a LHVI for a state Ψ then we have conclusively identified it as 'non-local'. However, if the no-go theorem does not apply to a particular state Φ, this does not allow us to conclude immediately that Φ is 'local'. It may be that there is some other no-go theorem which applies to Φ. For example, we have shown that given a basis structure Δ with a Z_4 phase group, the corresponding GHZ state Φ_Δ can have no LHVI: thus the Z_4 phase group is in some sense a marker of 'non-locality'. We also showed that an analogous no-go theorem fails if the phase group is $Z_2 \times Z_2$. But clearly from this we cannot immediately conclude that a $Z_2 \times Z_2$ phase group is in some way 'local'. We can in fact come to this conclusion from the fact that a basis structure with a $Z_2 \times Z_2$ phase group *does* arise in the physical category of a theory which we know to be a hidden variable theory - the toy theory. To show that a state is local we need to demonstrate that a LHVI exists for it. This raises the question: is it possible to construct a LHVI directly from certain phase groups?

We have focussed on the phase group of the basis structure Δ, when trying to determine whether a GHZ state Ψ_Δ has a LHVI. However, as we saw in section 6.3.1, the key determinant of the forbidden outcome triples of Ψ_Δ is in fact the full basis structure monoid. In some cases, the phase group fully determines the monoid. This is the case for example when we have a *totally unbiased basis structure* $\Delta = \{A, \delta, \epsilon\}$, one for which all states on A are either eigenstates or unbiased states (this is proved in detail in [11]). The basis structures on the elementary objects of **Stab** and **Spek** are examples of this type. The forbidden outcome triples of totally unbiased basis structures are completely classified by Abelian groups. Totally unbiased basis structures which are furthermore 'qubit-like' i.e. with three mutually unbiased observables, each with two eigenstates, will have phase groups of four elements; there are only two Abelian groups of four elements, Z_4 and $Z_2 \times Z_2$, and thus the basis structures of **Stab** and **Spek** exhaust the possibilities for 'qubit-like' totally unbiased basis structures. More generally, in the case of basis structures which are *not* totally unbiased, we expect the phase group to give us only part of the story about forbidden outcome triples (an example of such a basis structure would be the one in **Hilb** from example 3.3.2). An obvious question is whether it is possible to give a more complete description of the locality or non-locality of a GHZ state by analysis of the corresponding monoid.

We have focussed throughout on whether the GHZ states of a theory have LHVIs or not. Of course, even if we showed explicitly that the GHZ states of a physical category did have LHVIs we would not have proved that the corresponding theory had a local hidden variable interpretation, since there might simply be some other state in the category which did not have an LHVI. Why the focus on GHZ states then? The answer to this is partly just that we know that they are involved in a celebrated no-go theorem, and we know how to treat them within the categorical framework. Additionally, we expect GHZ states (in the abstract sense) to be ubiquitous in the physical categories of quantum-like theories, since they derive from basis structures, and we expect basis structures to be a feature of such categories. A third reason is that GHZ states play a particularly important role in many of our key examples of physical categories for quantum-like theories. Both **Spek** and **Stab** are notable for the way in which they are defined: as the closure of a collection of generating objects and morphisms. Employing compact closed duality, and the dagger functor, every generator can be expressed as a state: the group elements each correspond to a bipartite state, ϵ to a single-system state, and δ to the GHZ state. The question arises, if all of these states can be shown to have LHVIs,

does every state in the theory have a LHVI? It seems likely that this is true, although proving it for certain requires an understanding of how local hidden variables determine the values of non-separable observables. If it is true, then, in theories like **Spek** and **Stab**, establishing that the GHZ state generator had an LHVI would go most of the way towards establishing that the entire theory could be modelled by hidden variables.

The GHZ state no-go proof is an 'all-or-nothing' proof in that certain combinations of measurement outcomes are totally forbidden by the QM predictions, but all hidden states predict that at least some of them will be realised. There also exist several no-go proofs which are more statistical in character: a hidden variable theory predicts the same measurement outcomes as quantum mechanics does, but the two theories disagree on the probabilities of outcomes. A famous example would be the proof involving the Bell inequalities. Would it be possible to treat such no-go theorems within the categorical framework? Certainly the framework lends itself more naturally to all-or-nothing proofs, because these require us only to consider the *possibilities* of measurement outcomes rather than the full generalised probabilities. Nevertheless this issue needs to be addressed if the categorical framework is to be able to give a full commentary on the issue of hidden variables.

Consideration of the phase groups of the basis structures of a theory apparently gives us information on whether or not that theory shares the non-local features of quantum mechanics. Could it also tell us whether that theory goes beyond QM in its degree of non-locality? Various authors have considered quantum-like theories with states which exhibit a greater degree of non-locality than is found in any genuine quantum state [3]. What features do the physical categories of such theories have? Do they have basis structures, and if so, do the phase groups or basis structure monoids tell us anything about the degree of non-locality which their states exhibit?

Appendix A

Proof of form of general Spek morphisms

Here we give the full proof of the general form of the morphisms of **Spek**. The proof is lengthy, and readers are advised first to study the proof sketch in section 4.2.3 to understand the overall structure of the proof. Some parts of that section are repeated here for convenience.

A.1 Preliminaries

First we need to refine the group of permutations on Ⅳ. Note from definition 4.1.1 that the generator $\delta_{\mathbf{Spek}}$ effectively partitions the elements of Ⅳ into two halves $\{1,2\}$ and $\{3,4\}$.

Definition A.1.1 A *phased* permutation is an element of S_4 which maps $\{1,2\}$ into $\{1,2\}$ and $\{3,4\}$ into $\{3,4\}$. There are four such permutations: the identity, (12)(3)(4), (1)(2)(34) and (12)(34). These permutations form a subgroup of S_4, termed the *phased subgroup*. All other permutations in S_4 are termed *unphased*.

Definition A.1.2 **Spek** diagrams which can be generated by composition, Cartesian product and relational converse from the generators $\delta_{\mathbf{Spek}}$, $\epsilon_{\mathbf{Spek}}$, and the four *phased* permutations will be termed *phased diagrams*. All other diagrams will be termed *non-phased diagrams*.

The 'phased' terminology is chosen because the phased subgroup turns out to be isomorphic to the phase group of $\delta_{\mathbf{Spek}}$. Only a subset of the morphisms of **Spek** correspond to phased diagrams, and these will be termed *phased morphisms*. The majority of **Spek** morphisms, which correspond only to non-phased diagrams, are termed *non-phased morphisms*. The general form of a phased morphism is much simpler than the general form of a non-phased morphism. In fact our proof splits into two major stages: we first derive the general form of a phased morphism, and then use this result in our derivation of the general form of a non-phased morphism.

We next detail what each of the stages involved in building up a **Spek**-diagram introduced in section 4.2.1 means in concrete terms for the corresponding relations. Henceforth, remembering the discussion in section 4.2.2, we will assume that the relation corresponding to any n-legged diagram is of type $\mathrm{I} \to \mathrm{IV}^n$.

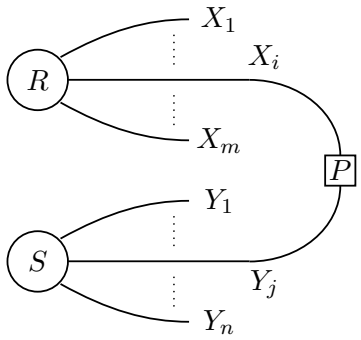
First, some preliminary definitions:

Definition A.1.3 The *i^{th}-remnant* of an n-tuple is the $(n-1)$-tuple obtained by deleting its i^{th} component.

Definition A.1.4 The *composite* of an m-tuple $(x_1, \ldots, x_m)$ and an n-tuple $(y_1, \ldots, y_n)$ is the $(m+n)$-tuple $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ from II^{m+n}.

Now what does the tree stage correspond to in relational terms?

Proposition A.1.5 Consider linking two diagrams, the first representing the relation $R : \mathrm{I} \to X_1 \times \cdots \times X_m$ the second representing the relation $S : \mathrm{I} \to Y_1 \times \cdots \times Y_n$ via a permutation P, to form a new diagram as shown:



(A.1)

The relation corresponding to this diagram is given by

$$* \sim \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m, y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n)\} \tag{A.2}$$

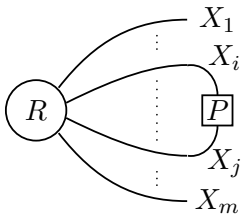
where $(x_1, \ldots, x_m) \in R(*)$, $(y_1, \ldots, y_n) \in S(*)$ and $x_i = P(y_j)$.

Or, in less formal language, for every pair of a tuple from R and a tuple from S obeying the condition $x_i = P(y_j)$, we form composite of the i^{th} remnant of the tuple from R, and the j^{th} remnant of the tuple from S.

Next, what does the loop stage correspond to in relational terms? Again we begin with a useful definition.

Definition A.1.6 The *i, j^{th}-remnant* of an n-tuple (where $i > j$) is the $(n-2)$-tuple obtained by deleting the j^{th} component of its i^{th}-remnant (or equivalently, deleting the $(i-1)^{\text{th}}$ component of its j^{th}-remnant).

Proposition A.1.7 Given a diagram representing the relation $R : \mathrm{I} \to X_1 \times \cdots \times X_m$, consider forming a new diagram by linking the i^{th} and j^{th} legs of the original diagram via a permutation P.



(A.3)

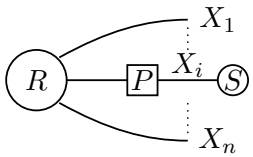
The relation corresponding to this diagram is given by:

$$* \sim \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m) | (x_1, \ldots, x_m) \in R(*), x_i = P(x_j)\} \tag{A.4}$$

Or, in less formal language, we take the i, j^{th}-remnant of every tuple for which $x_i = P(x_j)$.

Finally what does the capping stage correspond to in relational terms?

Proposition A.1.8 Consider linking two diagrams, the first representing the relation $R : \mathrm{I} \to X_1 \times \cdots \times X_n$ the second representing the relation $S : \mathrm{I} \to X_i$ via a permutation P, to form a new diagram as shown:



(A.5)

The relation corresponding to this diagram is given by:

$$* \sim \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) | (x_1, \ldots, x_n) \in R(*), x_i \in P(S(*))\} \tag{A.6}$$

Or, in less formal language, we take the i^{th} remnant of every tuple for which $x_i \in P(S(*))$.

Preliminaries complete we now proceed to the proof proper. We begin by deriving the general form of phased morphisms.

A.2 MiniSpek

We build up to the full theorem via a simplified case. For this we need a new category.

Definition A.2.1 The category **MiniSpek** is a subcategory of **FRel**. It is defined constructively, as follows:

- The objects of **MiniSpek** are the single-element set $\mathrm{I} = \{*\}$, the two element set $\mathbb{I} := \{0, 1\}$, and its n-fold Cartesian products $\mathbb{I}^n$.

- The morphisms of **MiniSpek** are all those relations generated by composition, Cartesian product and relational converse from the following generating relations:
  1. All permutations $\{\sigma_i : \mathbb{II} \to \mathbb{II}\}$ of the two element set. There are 2 such permutations, the identity and the operation which swaps the elements of $\mathbb{II}$. Together they form the group, Z_2.
  2. A relation $\delta_{\mathbf{Mini}} : \mathbb{II} \to \mathbb{II} \times \mathbb{II}$ defined by:
  $$0 \sim \{(0,0),(1,1)\} \qquad 1 \sim \{(0,1),(1,0)\}\,;$$
  3. a relation $\epsilon_{\mathbf{Mini}} : \mathbb{II} \to \mathrm{I} :: 0 \sim *$

Next we determine the general form of the relations which constitute the morphisms of **MiniSpek**. All of the considerations laid out in sections 4.2.1 and 4.2.2 also apply in this case.

Definition A.2.2 An element of $\mathbb{II}^n$ has *odd* parity if it has an odd number of '1' elements, and has *even* parity if it has an even number of '1' elements.

Whether an odd-parity n-tuple has an odd or even number of '0' elements clearly depends on whether n itself is odd or even. We could have chosen either 0 or 1 to play the role of labelling the parity; we have chosen 1 since it will turn out to be more convenient later on.

Theorem A.2.3 The relation in **MiniSpek** corresponding to an n-legged **MiniSpek**-diagram is a subset of $\mathbb{II}^n$, consisting of 2^{n-1} n-tuples, all of the same parity. The product of all the permutations appearing in the diagram determines the parity of the morphism: if the product is the identity (1)(2), the parity is even, if the product is (12) the parity is odd.

Several preliminary results are required for the proof of this theorem. First recall that $\mathbb{II}^n$ has 2^n elements: all possible n-tuples whose entries are either 0 or 1.

Some notation: we will use P to represent a particular parity, odd or even, and P' will represent the opposite parity.

Proposition A.2.4 There are equal numbers of odd- and even-parity tuples in $\mathbb{II}^n$: 2^{n-1} of each.

Proposition A.2.5 Consider the 2^{n-1} elements of $\mathbb{II}^n$ of a given parity P. Half of these n-tuples have a 0 in the i^{th} position, the other half have a 1 in the i^{th} position.

Proposition A.2.6 Consider an element of $\mathbb{II}^n$ of parity P. If its i^{th} component is 0, its i^{th}-remnant is of parity P. If its i^{th} component is 1, its i^{th}-remnant is of parity P'.

Proposition A.2.7 The composite of two tuples of opposite parity is of odd parity itself. The composite of two tuples of the same parity is of even parity itself.

Proposition A.2.8 Consider the set of all elements of $\mathbb{II}^n$ of parity P, with a 0 in the i^{th} position. Their i^{th}-remnants comprise the set of all elements of $\mathbb{II}^{n-1}$ of parity P. Likewise, the i^{th}-remnants of the set of all elements of $\mathbb{II}^n$ of parity P, with a 1 in the i^{th} position comprise the set of all elements of $\mathbb{II}^{n-1}$ of parity P'.

Proof: First consider the set of all elements of $\mathbb{II}^n$ of parity P, with a 0 in the i^{th} position. From proposition A.2.5 there are 2^{n-2} such elements. They are all different, but all have the same i^{th} component. Thus they must all differ at other positions, and thus their i^{th}-remnants are all distinct. From proposition A.2.6 they all have parity P. Thus the i^{th}-remnants comprise 2^{n-2} distinct $(n-1)$-tuples of parity P. From proposition A.2.4 we conclude that they constitute all elements of $\mathbb{II}^{n-1}$ of parity P. The proof for elements of $\mathbb{II}^n$ with a 1 in the i^{th} position proceeds analogously. □

Lemma A.2.9 Consider two **MiniSpek**-diagrams D_1 and D_2, and assume that the corresponding states ψ_1 and ψ_2 are of the form described in theorem A.2.3. Further assume that $\psi_1 \subset \mathbb{II}^m$ and has parity P_1, while $\psi_2 \subset \mathbb{II}^n$ and has parity P_2. Connecting the i^{th} leg of D_1 with the j^{th} leg of D_2, via a permutation S gives a new diagram, D_3. The state corresponding to D_3 is a subset of $\mathbb{II}^{m+n-2}$, consisting of 2^{m+n-3} $(m+n-2)$-tuples, all with parity P_3. P_3 depends on P_1, P_2 and S, in the following fashion:

	$P_1 = P_2$	$P_1 = P_2'$
$S = (1)(2)$	EVEN	ODD
$S = (12)$	ODD	EVEN

The state corresponding to D_3 will thus also take the form described in theorem A.2.3.

Proof: Consider ψ_1. From proposition A.2.5 it consists of 2^{m-2} tuples with 0 in the i^{th} position, and 2^{m-2} tuples with 1 in the i^{th} position. Removing the 0 and 1 from i^{th} position of these tuples yields respectively the *0-i^{th}-remnants* and the *1-i^{th}-remnants* of ψ_1. From proposition A.2.8 we conclude that they are all distinct.

Likewise ψ_2 includes 2^{n-2} tuples with S(0) in the j^{th} position and 2^{n-2} tuples with S(1) in the j^{th} position. Removing the S(0) and S(1) from j^{th} position of these tuples yields respectively the *S(0)-j^{th}-remnants* and the *S(1)-j^{th}-remnants* of ψ_2. From proposition A.2.8 we conclude that they are all distinct.

From proposition A.1.5 we know that ψ_3 will consist of all possible composites of the 0-i^{th}-remnants of ψ_1 with the S(0)-j^{th}-remnants of ψ_2, of which there are 2^{m+n-4}, and all possible composites of the 1-i^{th}-remnants of ψ_1 with the S(1)-j^{th}-remnants of ψ_2, of which there are also 2^{m+n-4}. The resulting $(m+n-2)$-tuples are clearly all different. In total then ψ_3 will consist of 2^{m+n-3} $(m+n-2)$-tuples.

We now consider the parities of the resulting tuples. From proposition A.2.6, the parity of the 0-i^{th}-remnants and the 1-i^{th}-remnants of ψ_1 are P_1 and P_1' respectively.

- If S is the identity then the parities of the S(0)-j^{th}-remnants and the S(1)-j^{th}-remnants of ψ_2 are P_2 and P_2' respectively. In this case, applying proposition A.2.7, if $P_1 = P_2$ then the tuples of ψ_3 are all of even parity, while if $P_1 = P_2'$ they are all of odd parity.
- If S is instead the permutation which swaps 0 and 1, then the parities of the S(0)-j^{th}-remnants and the S(1)-j^{th}-remnants of ψ_2 are P_2' and P_2 respectively. In this case, again applying proposition A.2.7, if $P_1 = P_2$ then the tuples of ψ_3 are all of odd parity, while if $P_1 = P_2'$ they are all of even parity.

□

Proposition A.2.10 Consider the 2^{n-1} elements of $\mathbb{I}^n$ of a given parity P. One quarter of these have a 0 in both the i^{th} and j^{th} positions, one quarter have a 0 in the i^{th} position and a 1 in the j^{th} position, one quarter have a 1 in the i^{th} position and a 0 in the j^{th} position, and the final quarter have a 1 in both the i^{th} and j^{th} positions.

Proof: Simple consequence of propositions A.2.5 and A.2.8. □

Proposition A.2.11 Consider the set of all elements of $\mathbb{I}^n$ of parity P with 0 in the i^{th} and j^{th} positions. Consider also the set of all elements of $\mathbb{I}^n$ of parity P with 1 in the i^{th} and j^{th} positions. The sets of i, j^{th} remnants of these two sets coincide: they comprise the set of all 2^{n-3} elements of $\mathbb{I}^{n-2}$ of parity P. An analogous results holds for those elements whose i^{th} and j^{th} components differ: their i, j^{th} remnants comprise the set of all 2^{n-3} elements of $\mathbb{I}^{n-2}$ of parity P'.

Proof: Simple consequence of propositions A.2.5, A.2.6 and A.2.8. □

Lemma A.2.12 Consider a **MiniSpek**-diagram D, and assume that the corresponding state ψ is of the form described in theorem A.2.3, is an element of $\mathbb{I}^m$ and has parity P. Connecting the i^{th} and j^{th} legs of D, via a permutation S yields a new diagram, D'. The state corresponding to D' is a subset of $\mathbb{I}^{m-2}$, consisting of 2^{m-3} $(m-2)$-tuples, all with parity $S(P)$.

Proof: From proposition A.2.10 we note that of the 2^{m-1} tuples in ψ, 2^{m-2} have identical i^{th} and j^{th} components, and 2^{m-2} have different i^{th} and j^{th} components. Removing the i^{th} and j^{th} components of these two classes yields respectively the *matching-i, j^{th}-remnants* and *nonmatching-i, j^{th}-remnants* of ψ. From proposition A.2.11 we know that each of these sets have 2^{n-3} distinct members.

From proposition A.2.6 and definition A.1.6, we can deduce that if the i^{th} and j^{th} components of a tuple of parity P are equal its i, j^{th}-remnant has parity P, whilst if its i^{th} and j^{th} components are not equal its i, j^{th}-remnant has parity P'. Thus the matching-i, j^{th}-remnants of ψ have parity P, while the nonmatching-i, j^{th}-remnants have parity P'.

From proposition A.1.7 we know that:

- If S is the identity then ψ' will consist of all the matching-i, j^{th}-remnants of ψ: there are 2^{m-3} distinct ones, all with parity P.

- If S is instead the permutation which swaps 0 and 1, then ψ' will consist of all the nonmatching-i, j^{th}-remnants of ψ: there are 2^{m-3} distinct ones, all with parity P'.

□

Lemma A.2.13 Consider a **MiniSpek**-diagram D, and assume that the corresponding state ψ is of the form described in theorem A.2.3, is an element of $\mathbb{II}^m$ and has parity P. Now consider the diagram D' that results when we cap off the i^{th} leg of D with the diagram representing $\epsilon_{\textbf{Mini}}$ (recall definition A.2.1), via a permutation S. The state ψ' corresponding to D' is a subset of $\mathbb{II}^{m-1}$, consisting of 2^{m-2} tuples, all with parity $S(P)$.

Proof: From proposition A.1.8 and definition A.2.1, ψ' consists of the i^{th}-remnants of all tuples in ψ for which $S(x_i) = 0$. From proposition A.2.8 we conclude that these constitute the set of all elements of $\mathbb{II}^{m-1}$ of parity P, if S is the identity, or of parity P' if S is the permutation which swaps 0 and 1. □

We are now finally in a position to prove theorem A.2.3.

Proof: In section 4.2.1 we showed that any **MiniSpek**-diagram can be built up beginning from the diagram representing the generating morphism $\delta_{\textbf{MiniSpek}}$, via three stages: linking diagrams together by external legs, via a permutation, to form a *tree-level* diagram with no internal loops; linking together external legs of a tree-level diagram, via a permutation, to form a *loop-level* diagram with internal loops; and finally capping off external legs with the diagram representing $\epsilon_{\textbf{MiniSpek}}$, via a permutation, to form a *capping-level* diagram. We prove the theorem by induction over these stages.

The base case is the diagram corresponding to the relation $\delta_{\textbf{Mini}}$. By bending around the input line we can convert this to a relation of type $\mathrm{I} \to \mathbb{II} \times \mathbb{II} \times \mathbb{II}$ which according to lemma 4.2.2 is the following subset of $\mathbb{II}^3$: $\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$. This clearly satisfies the inductive hypothesis.

Lemma A.2.9 shows that if two diagrams D_1 and D_2 both obey the inductive hypothesis, so does the tree-level diagram formed by linking them together along an external leg from each diagram, via a permutation.

Lemma A.2.12 shows that if a diagram D obeys the inductive hypothesis, so does the loop-level diagram formed by linking together two of the external legs of D, via a permutation.

Lemma A.2.13 shows that if a diagram D obeys the inductive hypothesis, so does the capping level diagram formed by capping off one of the external legs with the diagram corresponding to $\epsilon_{\textbf{Mini}}$, via a permutation. □

A.3 The general form of phased morphisms

We want to apply our results on **MiniSpek** to the category of real interest, **Spek**. To do this we first need to digress to discuss some features of relations.

Suppose we can partition a set A into m subsets A_i, and a set B into n subsets B_j. Recalling that a relation $R : A \to B$ is a subset of $A \times B$, it's clear that we can decompose R into mn components of the form $R_{i,j} : A_i \to B_j$, such that $R = \bigsqcup_{i,j} R_{i,j}$.

Definition A.3.1 The relations $R_{i,j} : A_i \to B_j$ are termed the *components* of R *with respect to the partitions* $A = \sqcup_i A_i$, $B = \sqcup_j B_j$.

Proposition A.3.2 Given four sets each with a partition $A = \sqcup_i A_i$, $B = \sqcup_j B_j$, $C = \sqcup_k C_k$ and $D = \sqcup_l D_l$, and three relations $R : A \to B$, $S : B \to C$ and $T : C \to D$:

1. The components of $(S \circ R) : A \to C$ are:

$$(S \circ R)_{i,k} = \bigsqcup_j S_{j,k} \circ R_{i,j} \tag{A.7}$$

2. The components of $(R \times T) : A \times B \to C \times D$ are:

$$(R \times T)_{i,j,k,l} = T_{k,l} \times R_{i,j} \tag{A.8}$$

3. The components of the relational converse $R^c : B \to A$ are:

$$R^c_{j,i} = (R_{i,j})^c \tag{A.9}$$

Consider a set A partitioned into two subsets A_1 and A_2. We can write A^m in terms of its subsets as some kind of binomial expansion:

$$A_1^m \sqcup (A_1^{m-1} \times A_2) \sqcup (A_1^{m-2} \times A_2 \times A_1) \sqcup \cdots \sqcup (A_1^{m-2} \times A_2^2) \sqcup \cdots \sqcup A_2^m \tag{A.10}$$

Definition A.3.3 Consider a relation $R : A^m \to A^n$ with the property that with respect to the decomposition $A = A_1 \sqcup A_2$ there are only two non-empty component relations: $R_1 : A_1^m \to A_1^n$ and $R_2 : A_2^m \to A_2^n$. Such a relation is *parallel* with respect to this partition of A.

Proposition A.3.4 Consider three relations $R : A^m \to A^n$, $S : A^n \to A^p$ and $T : A^p \to A^q$ which are all parallel with respect to the partition $A = A_1 \sqcup A_2$. The following relations:

$$\begin{aligned} S \circ R : &\quad A^m \to A^p \\ T \times R : &\quad A^{m+p} \to A^{n+q} \\ R^c : &\quad A^n \to A^m \end{aligned} \tag{A.11}$$

are all also parallel to the same partition of A.

Proof: Straightforward consequence of A.3.2. □

Finally we can use these results to make a connection between **MiniSpek** and **Spek**.

Proposition A.3.5 The generators of the phased morphisms of **Spek**, i.e. $\delta_{\mathbf{Spek}}$, $\epsilon_{\mathbf{Spek}}$ and the phased permutations on IV, are all parallel with respect to the following partition of $\mathrm{IV} = \{1,2\} \sqcup \{3,4\}$. We conclude that all phased morphisms of **Spek** are also parallel with respect to this partition. We refer to the two components of a phased **Spek** morphism as its $\{1,2\}$-component and $\{3,4\}$-component.

Proof: Straightforward verification combined with proposition A.3.4. □

Proposition A.3.6 The $\{1,2\}$-components of the generators of the phased morphisms of **Spek** are simply the generators of **MiniSpek** with the elements of $\mathrm{II} = \{0,1\}$ re-labelled according to $0 \mapsto 1$, $1 \mapsto 2$. Similarly the $\{3,4\}$-components of the generators of the phased morphisms of **Spek** are simply the generators of **MiniSpek** with the elements of $\mathrm{II} = \{0,1\}$ re-labelled according to $0 \mapsto 3$, $1 \mapsto 4$.

Proposition A.3.7 A state $\psi \subset \mathrm{IV}^n$ corresponding to a phased **Spek** diagram D is equal to the union of two states $\psi^{12} \subset \{1,2\}$ and $\psi^{34} \subset \{3,4\}$. ψ^{12} and ψ^{34} are obtained by the following procedure. Form a **MiniSpek** diagram D^{12} by replacing every incidence of $\delta_{\mathbf{Spek}}$ and $\epsilon_{\mathbf{Spek}}$ in D with $\delta_{\mathbf{Mini}}$ and $\epsilon_{\mathbf{Mini}}$, and replacing every incidence of a permutation with its $\{1,2\}$ component, re-labelled as a **MiniSpek** permutation as described in proposition A.3.6. Form a second **MiniSpek** diagram D^{34} in the obvious analogous fashion using $\{3,4\}$ components of permutations. ψ^{12} and ψ^{34} are the states corresponding to D^{12} and D^{34}, once again under the re-labelling described in proposition A.3.6.

Note that D^{12} and D^{34} will appear identical as graphs, both to each other and to D, but the labels on some of their permutations will differ.

Finally we are able to state our main result:

Theorem A.3.8 A phased morphism in **Spek** of type $\mathrm{I} \to \mathrm{IV}^n$ is a subset of IV^n, consisting of 2^n n-tuples, divided into two classes of equal number:

- The first class consists of tuples of 1s and 2s, all of either odd or even parity.
- The second class consists of tuples of 3s and 4s, again all of either odd or even parity.

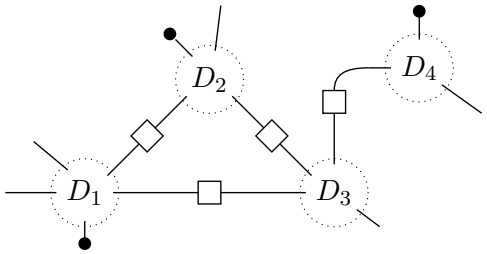
Proof: Straightforward consequence of proposition A.3.7 and theorem A.2.3. □

Note that we are adopting the convention that tuples of the first class have odd parity if they have an odd number of 2s, even parity if they have an even number of 2s. Tuples of the first class have odd parity if they have an odd number of 4s, even parity if they have an even number of 4s.

A.4 The general form of non-phased morphisms

We now proceed to derive the general form of the relations which constitute the morphisms of **Spek**. We have already derived the general form of those morphisms which correspond to diagrams in which the only permutations to appear are the four members of the phase subgroup. We now turn our attention to all other morphisms, those which don't have a diagrammatic counterpart involving only members of the phase subgroup. The general form of these morphisms is rather more complicated.

First note that a non-phased diagram can be built up in tree, loop and capping phases, analogous to our discussion in section 4.2.1, but in this case our basic units are not the three-legged $\delta_{\mathbf{Spek}}$ diagrams, but complete n-legged phased diagrams, and the permutations joining them are not members of the phase subgroup.



(A.12)

These phased sub-diagrams will be termed *zones*. A general **Spek** diagram consists then of phased zones linked by non-phased permutations. We now have the vocabulary to state the general form of relation corresponding to such diagrams.

Definition A.4.1 An *external zone* in a **Spek**-diagram is a zone with external legs.

Theorem A.4.2 The relation in **Spek** corresponding to an n-legged **Spek**-diagram with m external zones is *either*

A subset of IV^n satisfying the following properties:

1. It contains 2^n n-tuples.
2. Each n-tuple is divided into m sub-tuples, each corresponding to an external zone in the diagram. Each sub-tuple has as many components as the corresponding zone has external legs - we will denote this number by n_i - and has a well-defined *type* (components either all 1 or 2, or all 3 or 4) and *parity* (as defined for phased relations).
3. The 2^n tuples are grouped into 2^m equally sized subsets called *blocks*. The i^{th} sub-tuple of every tuple in a block has the same type and parity. The sequence of types and parities of each sub-tuple is called the *signature* of the block. Each block has a unique signature.
4. Each block has $2^{(n-m)}$ elements: these constitute every possible combination of the sub-tuples which satisfy the parity and type requirements of the block's signature.

5. Each of the four possible combinations of parity and type appear in the i^{th} sub-tuple in one quarter of the tuples.

or it is equal to the empty set, $\emptyset$.

A couple of remarks on notation and terminology first. The sub-tuples referred to in point (2) above, corresponding to zones in the diagram, may also be termed *zones* themselves. Whether we are referring to a zone of a diagram, or zone of a tuple should be clear from the context. We represent the signature of a tuple with m zones as $(P_1, T_1; \ldots; P_m, T_m)$ where P_i is the parity of the i^{th} zone, and T_i is its type. Again, if P is a parity, P' indicates the opposite parity, and likewise if T is a type ((12) or (34)), T' represents the other type.

The proof of this theorem will require many intermediate results.

A.4.1 Tree-level diagrams

Lemma A.4.3 Consider an n-legged non-phased diagram D_1 with m zones. Suppose the corresponding state $\psi_1 \subset \text{IV}^n$ satisfies the conditions in theorem A.4.2. Now consider linking the i^{th} leg of D_1 to the j^{th} leg of an n'-legged phased diagram D_2 (with corresponding state ψ_2), via a non-phased permutation S, to create an $(n+n'-2)$-legged diagram D_3 with $m+1$ zones. We will assume that the i^{th} leg of D_1 lies within its k^{th} external zone. The state $\psi_3 \subset \text{IV}^{n+n'-2}$ corresponding to D_3 also satisfies the conditions in theorem A.4.2.

Proof: We will go step by step through the conditions from theorem A.4.2. First, condition (1), ψ_3 should comprise $2^{n+n'-2}$ tuples. We define the 1-, 2-, 3- and 4-i^{th}-remnants of ψ_1 in straightforward analogy with the 0- and 1-i^{th}-remnants defined in the proof of lemma A.2.9. From proposition A.1.5 we know that the elements of ψ_3 comprise all the possible composites of the x-i^{th}-remnants of ψ_1 and the $S(x)$-j^{th}-remnants of ψ_2, where $x = 1, \ldots, 4$. By hypothesis (point 5 in theorem A.4.2) there will be equal numbers of 1-, 2-, 3- and 4-i^{th}-remnants of ψ_1, 2^{n-2} of each. And from proposition A.2.5 and theorem A.3.8 there will be equal numbers of 1-, 2-, 3- and 4-j^{th}-remnants of ψ_2, $2^{n'-2}$ of each. Thus there are $2^{n+n'-4}$ distinct composites of the x-i^{th}-remnants of ψ_1 and the $S(x)$-j^{th}-remnants of ψ_2, and in total ψ_3 contains $4 \times 2^{n+n'-4} = 2^{n+n'-2}$ tuples.

Next, condition (2), the tuples of ψ_3 should have as many sub-tuples as D_3 has external zones. If the external zone in D_1 to which we are linking D_2 has only one external leg, then it will no longer be an external zone in the new diagram D_3. In this case the corresponding sub-tuple in ψ_1 will have only one component. This block will not appear in the i^{th}-remnants of ψ_1, which will then have $m-1$ sub-tuples. If the linking zone has more than one external leg, it will continue to be an external zone in D_3, and the i^{th}-remnants of ψ_1 will have m sub-tuples. From proposition A.2.8 we deduce that the x-j^{th}-remnants of ψ_2 all have definite type and parity. Thus, in the composites which constitute ψ_3, the x-j^{th}-remnant of ψ_2 comprises a single zone, corresponding to the extra zone in D_3 formed by the phased diagram D_2[1]. We

[1]We neglect the possibility that D_2 has only one external leg, since this contingency will be covered in the capping stage.

will conventionally consider this to be the $(m+1)^{\text{th}}$ zone of the tuples in ψ_3. We thus conclude that the tuples of ψ_3 have the same number of sub-tuples as D_3 has external zones, $m+1$ if the linking zone in D_1 has more than one external leg, m if it has only one.

Next, condition (3), ψ_3 should consist of 2^{m+1} blocks all with unique signatures. Consider a block $B \subset \psi_1$, with signature $(P_1, T_1; \ldots; P_k, T_k; \ldots; P_m, T_m)$, in which, for definiteness we assume that the k^{th} zone is of type-(12) (the argument runs entirely analogously if it is of type-(34)). The composites of the 1-i^{th}-remnants of B and the $S(1)$-j^{th}-remnants of ψ_2 all have the same signature, $(P_1, T_1; \ldots; P_k, T_k; \ldots; P^1_{m+1}, T^1_{m+1})$. They constitute a block $B_1 \subset \psi_3$. The composites of the 2-i^{th}-remnants of B and the $S(2)$-j^{th}-remnants of ψ_2 also all have the same signature, $(P_1, T_1; \ldots; P'_k, T_k; \ldots; P^2_{m+1}, T^2_{m+1})$. They constitute a block $B_2 \subset \psi_3$. (The relationship between P^1_{m+1} and P^2_{m+1}, and T^1_{m+1} and T^2_{m+1} depends on the permutation S). We term B the *parent* block, and B_1 and B_2 the *progeny* blocks. Suppose a parent block $B' \subset \psi_1$, distinct from B, gave rise to a progeny block B'_1 with the same signature at B_1, $(P_1, T_1; \ldots; P_k, T_k; \ldots; P^1_{m+1}, T^1_{m+1})$. To be distinct from B, B' would have to have a signature of $(P_1, T_1; \ldots; P'_k, T_k; \ldots; P_m, T_m)$, with B'_1 deriving from its 2-i^{th}-remnant. But in this case the signature of B'_1's $(m+1)^{\text{th}}$ zone would be (P^2_{m+1}, T^2_{m+1}). Thus we conclude that all progeny blocks in ψ_3 derived from parent blocks in ψ_1 are distinct, and the number of blocks in ψ_3 is double that in ψ_1.

Next, condition (4), a block of ψ_3 should contain all possible combinations of zones whose parity and type are consistent with its signature. With no loss of generality we will work with the blocks from the previous paragraph. By hypothesis and by proposition A.2.8 the 1-i^{th}-remnants of B will constitute all possible $(n-1)$-tuples of signature $(P_1, T_1; \ldots; P_k, T_k; \ldots; P_m, T_m)$. Again, by proposition A.2.8 the $S(1)$-j^{th}-remnants of ψ_2 will constitute all possible $(n'-1)$-tuples of parity P^1_{m+1} and type T^1_{m+1}. The elements of B_1 are all possible composites of the 1-i^{th}-remnants of B and the $S(1)$-j^{th}-remnants of ψ_2. Thus B_1 satisfies condition (4). A similar argument applies to B_2.

□

Corollary A.4.4 All tree-level **Spek**-diagrams satisfy the conditions in theorem A.4.2.

Proof: Note from theorem A.3.8 that the general form of phased morphisms satisfies the conditions in theorem A.4.2. In this case $m = 1$, and we have two blocks, and just a single zone - the tuple itself. Any tree-level **Spek**-diagram can be constructed step-by-step, beginning with a single phased diagram, by adding another phased diagram to the existing diagram via an unphased permutation at each step. Lemma A.4.3 shows that after each stage of this process the state corresponding to the resulting diagram still satisfies the conditions in theorem A.4.2. □

A.4.2 Totally and partially unphased permutations

Before proceeding we need to further refine our classification of permutation. Formally we distinguished between phased and unphased permutations. We now divide the unphased permutations into two classes.

Definition A.4.5 A *totally unphased* (TU) permutation is an element of S_4 which maps $\{1,2\}$ into $\{3,4\}$ and vice versa. There are four such permutations: (13)(24), (14)(23), (1324) and (1423).

Definition A.4.6 A *partially unphased* (PU) permutation is an element of S_4 which either maps 1 into $\{1,2\}$ and 2 into $\{3,4\}$ or vice versa, *and* which either maps 3 into $\{1,2\}$ and 4 into $\{3,4\}$ or vice versa. Any permutation which is not phased or totally unphased is partially unphased. There are 16 such permutations.

Proposition A.4.7 Suppose we link a **Spek**-diagram D_1 with m zones, with corresponding state ψ_1, from its k^{th} zone, via a permutation S, to a phased diagram D_2 with corresponding state ψ_2, to form a diagram D_3 with corresponding state ψ_3. Consider a parent block $B \subset \psi_1$, with type signature $(T_1, \ldots, T_k, \ldots, T_m)$. The signatures of the two progeny blocks B_1 and B_2 will be:

- If S is TU: $(T_1, \ldots, T_k, \ldots, T_m, T'_k)$ for B_1 and B_2.
- If S is PU: $(T_1, \ldots, T_k, \ldots, T_m, T_k)$ for B_1 and $(T_1, \ldots, T_k, \ldots, T_m, T'_k)$ for B_2.

A.4.3 Loop-level: preliminaries

We now move on to the loop level. First we need to introduce the important notion of *chains*.

Definition A.4.8 Two zones in a **Spek**-diagram are *adjacent* if they are directly linked via a permutation. Two sub-tuples in the corresponding state are adjacent if they correspond to adjacent zones.

Definition A.4.9 A *chain* in a **Spek**-diagram is a sequence of adjacent zones. A chain in the corresponding state is the sequence of sub-tuples corresponding to the zones in the chain. An *n-chain* is a chain with n zones.

Definition A.4.10 Consider a diagram D with a chain, with corresponding state ψ. The *end-type* of a block $B \subset \psi$ with respect to the chain refers to the combination of the types of the initial and final zones of the chain. Clearly there are four possible end-types.

Definition A.4.11 In a block $B \subset \psi$ which is *same-ended* with respect to a chain, the initial and final zones of the chain have the same type. A *different-ended* block is defined analogously.

Clearly any loop in a diagram is formed by linking together the initial and final zones of a chain via an unphased permutation.

Definition A.4.12 The *x, y-i, j^{th}-remnants* of a set of tuples are the i, j^{th}-remnants of all those tuples with x in the i^{th} position and y in the j^{th} position.

Suppose we close a chain in a diagram D with corresponding state ψ, to form a diagram D' with corresponding state ψ'. From proposition A.1.7, ψ' consists of the $x, S(x)$-i, j^{th}-remnants of ψ. We will need various properties of these remnants.

Proposition A.4.13 If the signature of some tuple is $(P_1, T_1; \ldots; P_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m)$ then the signature of its i, j^{th}-remnant can take one of four forms:

- $(P_1, T_1; \ldots; P_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m)$ if the i^{th} component is 1 or 3 and the j^{th} component is 1 or 3.
- $(P_1, T_1; \ldots; P_k, T_k; \ldots; P'_l, T_l; \ldots; P_m, T_m)$ if the i^{th} component is 1 or 3 and the j^{th} component is 2 or 4.
- $(P_1, T_1; \ldots; P'_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m)$ if the i^{th} component is 2 or 4 and the j^{th} component is 1 or 3.
- $(P_1, T_1; \ldots; P'_k, T_k; \ldots; P'_l, T_l; \ldots; P_m, T_m)$ if the i^{th} component is 2 or 4 and the j^{th} component is 2 or 4.

We use a, a' to denote the two distinct elements of T_k, either 1 and 2, or 3 and 4, depending on the type. Likewise b, b' denote the two distinct elements of T_l. If $T_k = T_l$ we will adopt the convention that $a = b, a' = b'$.

Proposition A.4.14 Of the 2^{n-m} tuples in some block $B \in \psi$, one quarter have an a in the i^{th} position and a b in the j^{th} position, one quarter have an a in the i^{th} position and a b' in the j^{th} position, one quarter have an a' in the i^{th} position and a b in the j^{th} position, and the last quarter have an a' in the i^{th} position and a b' in the j^{th} position.

Proof: Suppose in any tuple in ψ the i^{th} component is in the k^{th} zone, and the j^{th} component is in the l^{th} zone. Let P_k and P_l be the parities of these zones in block B. From proposition A.2.5, half of the possible k^{th} sub-tuples will have an a in the i^{th} position, and half will have a'. Similarly half of the possible l^{th} sub-tuples will have an b in the j^{th} position, and half will have b'. By hypothesis (condition 4 in theorem A.4.2) B contains tuples featuring every possible combination of k^{th} sub-tuple with parity P_k, and l^{th} sub-tuple with parity P_l, thus completing the proof. □

The two cases of closing a chain via a partially unphased permutation and with a totally unphased permutation are distinct, and will be treated separately. We will begin with the simpler partially unphased case.

A.4.4 Closing chains with partially unphased permutations

Lemma A.4.15 Consider an n-legged D with m external zones, which contains a chain. The initial zone of the chain is the k^{th} zone of D, while its final zone is the l^{th} of D. Suppose the corresponding state ψ satisfies the conditions in theorem A.4.2. Now consider forming a new

$(n-2)$-legged diagram D', with corresponding state ψ', by linking the i^{th} leg of D, which is in the initial zone of the chain, to the j^{th} leg, which is in the final zone of the chain, via a *partially unphased* permutation S. ψ' also satisfies the conditions in theorem A.4.2.

The proof of this lemma requires some subsidiary results.

Proposition A.4.16 If S is partially unphased then each block $B \subset \psi$ gives rise to a single block $B' \subset \psi'$, consisting of 2^{n-m-2} tuples. We call B' the *progeny* block and B the *parent* block.

Proof: If S is partially unphased, then $S(a) = b$ or b' implies that $S(a') \neq b$ or b', and vice versa. Thus, from proposition A.4.14 we see that, in any given block $B \subset \psi$, only a quarter of the tuples 'yield' $x, S(x)$-i, j^{th}-remnants. Thus each B has 2^{n-m-2} $x, S(x)$-i, j^{th}-remnants. From proposition A.4.13 we note that each of these remnants has the same signature. Via a counting argument we conclude that the remnants represent all possible combinations of tuples of this signature - thus they constitute a single block $B' \subset \psi'$. □

Definition A.4.17 The relationship between the signatures of parent and progeny blocks will take one of the four forms appearing in proposition A.4.13. Which particular form is exhibited for a given parent block is termed the *parent-progeny-signature-relation* (PPSR) for that block.

Proposition A.4.18 All blocks with the same end-type relative to the chain will exhibit the same PPSR upon closing of the chain via a partially unphased permutation.

Proof: From definition A.4.6, if S is partially unphased then for each end-type there is only one value of x for which there are $x, S(x)$-i, j^{th}-remnants. Thus, for every block of a given end-type we are eliminating the same values to yield our $x, S(x)$-i, j^{th}-remnants, and thus, from proposition A.4.13 the PPSR is the same in each case. □

Proposition A.4.19 After closing a chain with a partially unphased permutation two distinct parent blocks $B_1, B_2 \subset \psi$ will give rise to distinct progeny blocks $B_1', B_2' \subset \psi'$.

Proof: From proposition A.4.13 we note that parent and progeny blocks have identical type signatures. Thus if B_1 and B_2 have distinct type signatures, so will B_1' and B_2'. If B_1 and B_2 have identical type signatures we can conclude (i) They will exhibit identical PPSRs; and (ii) If they are themselves distinct they must have distinct parity signatures. But clearly applying the same PPSR to two distinct parity signatures yields a further two distinct parity signatures: thus B_1' and B_2' are distinct. □

We can now prove lemma A.4.15

Proof: From proposition A.4.16 each block $B \subset \psi$ gives rise to one progeny block, $B' \subset \psi'$ consisting of 2^{n-m-2} tuples (satisfying condition 4 of theorem A.4.2). By hypothesis ψ consists

of 2^m blocks, thus so does ψ' (satisfying condition 3), and in total, ψ' consists of 2^{n-2} tuples (satisfying condition 1). From proposition A.4.13 we see that the number of zones in the tuples of ψ' is unchanged, so condition (2) is also satisfied.

□

A.4.5 Closing chains with totally unphased permutations

This is somewhat more complicated. In this section we will continue to use the terminology introduced in lemma A.4.15: we form diagram D' by closing a chain in diagram D, their corresponding states are ψ' and ψ, the initial and final zones of the chain are as described before; however, we will now assume that S is *totally unphased*.

First, recall the definition of blocks which are same-ended and different-ended with respect to a chain (definition A.4.11).

Proposition A.4.20 If S is totally unphased then a same-ended block $B \in \psi$ has no $x, S(x)$-i, j^{th}-remnants, and thus gives rise to no progeny blocks in ψ'.

Proposition A.4.21 If S is totally unphased then a different-ended block $B \subset \psi$, with signature $(P_1, T_1; \ldots; P_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m)$ gives rise to two progeny blocks $B_1, B_2 \subset \psi'$, each of which consists of 2^{n-m-2} tuples. The signatures of these blocks are either:

$$(P_1, T_1; \ldots; P_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m) \text{ and } (P_1, T_1; \ldots; P'_k, T_k; \ldots; P'_l, T_l; \ldots; P_m, T_m)$$

$$\text{or } (P_1, T_1; \ldots; P'_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m) \text{ and } (P_1, T_1; \ldots; P_k, T_k; \ldots; P'_l, T_l; \ldots; P_m, T_m)$$

Proof: Using the terminology of proposition A.4.14 either $S(a) = b, S(a') = b'$ or $S(a) = b', S(a') = b$. Either way in any given block $B \subset \psi$, one half of the tuples 'yield' $x, S(x)$-i, j^{th}-remnants. Thus each B has 2^{n-m-1} $x, S(x)$-i, j^{th}-remnants. Further it is clear that *either* half of these will all have the first signature listed in proposition A.4.13, and the other half will all have the fourth signature, *or* half will all have the second signature, and half will all have the third signature. □

Definition A.4.22 We define the parent-progeny-signature-relation (PPSR) for the case of closing with a totally unphased morphism exactly as we did for partially unphased morphisms (definition A.4.17). In this case there are clearly only two possible PPSRs.

Proposition A.4.23 All blocks with the same end-type relative to the chain will exhibit the same PPSR upon closing of the chain via a totally unphased permutation.

Proof: Totally analogous to proof of proposition A.4.18. □

Mirrored blocks and duplicated progeny blocks

Unlike the partially unphased case it is *not* generally true that progeny blocks from different parent blocks are themselves distinct. We will now show that parent blocks with a specific relationship will produce identical progeny blocks. Fortunately these are the only blocks which will produce identical progeny.

Definition A.4.24 Two blocks $B, B' \subset \psi$ are said to be *mirrored* with respect to the chain if their respective signatures are:

$$(P_1, T_1; \ldots; P_k, T_k; \ldots; P_l, T_l; \ldots; P_m, T_m) \text{ and } (P_1, T_1; \ldots; P'_k, T_k; \ldots; P'_l, T_l; \ldots; P_m, T_m)$$

where all zones not explicitly listed have identical parities and types. Together B and B' constitute a *mirrored pair*.

Proposition A.4.25 Two different-ended blocks $B, B' \subset \psi$, mirrored with respect to a chain, give rise to identical pairs of progeny blocks when the chain is closed via a totally unphased permutation.

Proof: B and B' have the same end-type with respect to the chain, and thus exhibit the same PPSR. Referring to proposition A.4.21, it is simple to see that, whichever PPSR it is, the two progeny blocks derived from B will have identical signatures to those derived from B'. □

Proposition A.4.26 If different-ended two blocks $B, B' \subset \psi$ are not mirrored with respect to a chain, then upon closing that chain with a totally unphased permutation they will give rise to distinct pairs of progeny blocks.

Proof: From proposition A.4.13 we note that parent and progeny blocks have identical type signatures. Thus if B and B' have distinct type signatures, so will their progeny blocks. If they have identical type signatures we conclude (i) They will exhibit identical PPSRs; and (ii) If they are themselves distinct they must have distinct parity signatures. If they are not mirrored, then (ii) implies that either the parities of their i^{th} zones differ and those of their j^{th} zones coincide, or vice versa. In either case, applying either PPSR to both can easily be seen to lead to distinct pairs of progeny blocks. □

When mirrored blocks arise

Proposition A.4.27 Consider a tree-level diagram D_1 (with corresponding state ψ_1) with an n-chain, whose initial and final zones are the k^{th} and l^{th} of D_1. Now consider extending the chain by adding a phased diagram D_2 (with corresponding state ψ_2) to the final zone of the chain, via a *totally unphased* permutation R to yield a diagram D_3 (with corresponding state ψ_3) with an $(n+1)$-chain. Consider two blocks $B, B' \in \psi_1$ which are mirrored with respect to the n-chain in D_1. B has two progeny blocks B_1 and B_2, B' has two progeny blocks B'_1 and B'_2. B_1 and B'_2 are mirrored with respect to the $(n+1)$-chain in D_3, as are B_2 and B'_1.

Proof: The signatures of B and B' are:

$$\begin{aligned} B: &\quad (P_1, T_1; \ldots, P_k, T_k; \ldots, P_l, T_l; \ldots, P_m, T_m) \\ B': &\quad (P_1, T_1; \ldots, P'_k, T_k; \ldots, P'_l, T_l; \ldots, P_m, T_m) \end{aligned}$$

where all components not explicitly written have identical parity and type.

Denote the two elements of T_l by a (representing either 1 or 3) and a' (representing either 2 or 4). The elements of $B_1(B'_1)$ are the composites of the a-i^{th}-remnants of $B(B')$ and the $R(a)$-j^{th}-remnants of ψ_2. The elements of $B_2(B'_2)$ are the composites of the a'-i^{th}-remnants of $B(B')$ and the $R(a')$-j^{th}-remnants of ψ_2. If R is totally unphased then both $R(a), R(a') \in T'_l$, and thus $R(a') = (R(a))'$. Taking all this into account we conclude that the signatures of the progeny blocks are:

$$\begin{aligned} B_1: &\quad (P_1, T_1; \ldots, P_k, T_k; \ldots, P_l, T_l; \ldots, P_m, T_m; P_{m+1}, T'_l) \\ B_2: &\quad (P_1, T_1; \ldots, P_k, T_k; \ldots, P'_l, T_l; \ldots, P_m, T_m; P'_{m+1}, T'_l) \\ B'_1: &\quad (P_1, T_1; \ldots, P'_k, T_k; \ldots, P'_l, T_l; \ldots, P_m, T_m; P_{m+1}, T'_l) \\ B'_2: &\quad (P_1, T_1; \ldots, P'_k, T_k; \ldots, P_l, T_l; \ldots, P_m, T_m; P'_{m+1}, T'_l) \end{aligned}$$

from which we can read off that B_1 and B'_2 are mirrored with respect to the $(n+1)$-chain, as are B'_1 and B_2. □

Proposition A.4.28 Consider a diagram D with a chain. Suppose the corresponding state ψ includes two blocks $B_1, B_2 \subset \psi$ which are mirrored with respect to the chain. Now we generate a new diagram D' either by adding a new zone to D, or by closing some other chain in D, but we *do not* either extend or close the original chain, which remains in D'. In all cases the progeny blocks of B_1 and B_2 will constitute one or two mirrored pairs.

Proof: Tedious calculation verifies this claim for all cases. □

Proposition A.4.29 Given any diagram with a chain in which all of the zones are linked via totally unphased permutations, the corresponding state will consist entirely of pairs of blocks which are mirrored with respect to the chain.

Proof: Consider a diagram consisting solely of a 2-chain, with its two zones joined via a totally unphased permutation. It is straightforward to verify that it will have four blocks, with signatures:

$$(P_A, T; P_C, T') \quad (P'_A, T; P'_C, T') \quad (P_B, T'; P_D, T) \quad (P'_B, T'; P'_D, T)$$

(to see this, note that a phased diagram has two blocks, with signatures (P_A, T) and (P_B, T')). Thus, such a 2-chain consists of two mirrored pairs. We then invoke proposition A.4.27 to show that we can extend the chain, *via totally unphased permutations* to any length and the resulting state will still consist of mirrored pairs. Finally we invoke proposition A.4.28 to show that adding any extra zones and closing any loops elsewhere in the diagram has no effect on this property. □

All-same and all-different chains

Definition A.4.30 An *all-same chain* in a **Spek**-diagram D is a chain such that in every block in the corresponding state ψ is same-ended (definition A.4.11). An *all-different chain* is defined similarly.

Proposition A.4.31 Extending an all-same chain via a totally unphased permutation results in an all-different chain. Extending an all-different chain via a totally unphased permutation results in an all-same chain.

Proof: Let the unextended n-chain lie within an m-legged diagram D, with corresponding state ψ. Let the first and n^{th} zones in the chain be the k^{th} and l^{th} zones in D respectively. Following the normal convention, the $(n+1)^{\text{th}}$ zone in the extended chain will be the $(m+1)^{\text{th}}$ zone in the extended diagram D', which has corresponding state ψ'.

Proposition A.4.7 indicates that a parent block in which the i^{th} and $(m+1)^{\text{th}}$ zones have the same type gives rise to two progeny blocks in which the i^{th} and $(m+1)^{\text{th}}$ zones have different types, and vice versa. Thus if all parent blocks have matching types, all progeny blocks will have different types, and vice versa. □

Proposition A.4.32 Consider a diagram D with an all-same n-chain. Now we generate a new diagram D' either by adding a new zone to D, or by closing some other chain in D, but we *do not* either extend or close the original chain, which remains as an n-chain in D'. This chain is still all-same. An exactly analogous result holds for an all-different chain.

Proof: From propositions A.4.21 and A.4.16 closing a loop anywhere in a diagram results in progeny blocks with type signatures identical to those of their parent blocks (aside from the case where closing with a totally unphased permutation leads to no progeny block). From proposition A.4.7 extending a diagram by adding a phased zone results in progeny blocks with type signatures which are identical to those of the parent blocks *when restricted to the zones from the parent diagram*. Since the chain is not being extended in this case, the types of its initial and final zones will be unaffected. □

Proposition A.4.33 In any tree-level or loop-level diagram a chain whose zones are linked only by *totally unphased* permutations is an all-same or all-different chain.

Proof: A diagram with such a chain can be built up by (i) linking together all the zones in the chain sequentially via totally unphased permutations, then (ii) by connecting all the zones which do not appear in the chain, and closing up any loops. The first step is to link two phased diagrams together via a totally unphased morphism to form a 2-chain. Using proposition A.4.7 we conclude that all such 2-chains are all-different. We then invoke proposition A.4.31 to conclude that by the end of stage (i) all chains will be either all-same or all-different. Proposition A.4.32 then shows that stage (ii) has no effect on the end-type of the chain. □

Finally we are able to state our key result on the effect of closing chains with totally unphased morpisms.

Lemma A.4.34 Consider an n-legged D with m external zones, which contains a chain *whose zones are linked only by totally unphased permutations.* The initial zone of the chain is the k^{th} zone of D, while its final zone is the l^{th} of D. Suppose the corresponding state ψ satisfies the conditions in theorem A.4.2. Now consider forming a new $(n-2)$-legged diagram D', with corresponding state ψ', by linking the i^{th} leg of D, which is in the initial zone of the chain, to the j^{th} leg, which is in the final zone of the chain, via a *totally unphased* permutation S. Either ψ' also satisfies the conditions in theorem A.4.2 or $\psi' = \emptyset$.

Note that this lemma is *almost* the equivalent of lemma A.4.15 for partially unphased permutations, except that there is a restriction on what kind of chains we are closing - those linked solely by totally unphased permutations.

Proof: Note first, from propositions A.4.29 and A.4.33 that if we have a diagram with a chain whose zones are linked only by totally unphased morphisms then (i) the chain is either all-same or all-different (ii) the state corresponding to the diagram consists entirely of pairs of blocks which are mirrored with respect to the chain.

From proposition A.4.20, we conclude that if the chain in D is all-same then no tuples in ψ have $x, S(x)$-i, j^{th}-remnants, and thus ψ' is empty.

If the chain is all-different, from proposition A.4.21 each block $B \subset \psi$ gives rise to two progeny blocks, $B_1, B_2 \subset \psi'$ each consisting of 2^{n-m-2} tuples. By hypothesis ψ consists of 2^m blocks, thus there are 2^{m+1} such progeny blocks. However, since ψ consists entirely of mirrored pairs of blocks, by proposition A.4.25, only 2^m of these blocks are distinct.

Thus in total, ψ' consists of 2^{n-2} tuples, thus satisfying condition (1) of theorem A.4.2. From proposition A.4.13 we see that the number of zones in the tuples of ψ' is unchanged, so condition (2) is also satisfied. Conditions (3) and (4) are satisfied via proposition A.4.21.

□

A.4.6 Loop level diagrams

Lemma A.4.35 All loop-level **Spek**-diagrams have one of the forms described in theorem A.4.2.

Proof: Any loop level diagram D can be formed in three stages: (i) Join all the zones together in a tree-level diagram; (ii) The chains giving rise to any loops in D whose zones are linked by at least one partially unphased morphism are now closed, *via a partially unphased morphism*; (iii) The chains giving rise to all remaining loops, i.e. those whose zones are linked only by totally unphased morphisms, are closed via a totally unphased morphism.

By corollary A.4.4 all tree-level diagrams satisfy the conditions in theorem A.4.2. By lemma A.4.15 subsequent to stage (ii) all diagrams will still satisfy these conditions. Finally lemma A.4.34 implies that subsequent to stage (iii) all diagrams will still satisfy the conditions, thus concluding the proof. □

A.4.7 Capping level diagrams

The final stage in constructing a **Spek** diagram involves capping off certain external legs with an $\epsilon_{\mathbf{Spek}}$ morphism, possibly via a permutation.

Lemma A.4.36 Consider an n-legged D with m external zones. Suppose the corresponding state ψ satisfies the conditions in theorem A.4.2. Now consider forming a new $(n-1)$-legged diagram D', with corresponding state ψ', by capping one of the external legs with an $\epsilon_{\mathbf{Spek}}$ morphism, via an unphased permutation S. ψ' also satisfies the conditions in theorem A.4.2.

Proof: By proposition A.1.8 ψ' will consist of the a- and b-i^{th}-remnants of ψ, where $a = S(1)$ and $b = S(3)$. By hypothesis (condition 5 of theorem A.4.2) half of the blocks $B \subset \psi$ have $T_k = T$ and half have $T_k = T'$.

If S is totally unphased then $a \in T$ and $b \in T'$. By proposition A.2.5 half of those blocks with $T_k = T$ will have a as their i^{th} component. By proposition A.2.8 the a-i^{th}-remnants of any such block will all have the same signature, and thus constitute a block of ψ' themselves. Likewise half of those blocks with $T_k = T'$ will have b as their i^{th} component, and their b-i^{th}-remnants constitute a block of ψ'. Thus, every block in ψ gives rise to one progeny block in ψ', containing 2^{n-m-1} tuples.

If S is partially unphased then $a, b \in T$. Those blocks with $T_k = T$ each generate two blocks, one deriving from the a-i^{th}-remnants, the other from the b-i^{th}-remnants. Each contains 2^{n-m-1} tuples. Those blocks with $T_k = T$ generate no progeny blocks.

In each case, ψ' has 2^m blocks, each containing 2^{n-m-1} tuples, and thus has 2^{n-1} tuples in total. The a- and b-i^{th}-remnants of ψ have the same zone structure as the tuples of ψ. Thus ψ' also satisfies the conditions in theorem A.4.2. □

Finally we can give a proof of theorem A.4.2:

Proof: Any **Spek** diagram can be formed by capping off external legs of a loop-level diagram with $\epsilon_{\mathbf{Spek}}$ morphisms. By lemma A.4.35 the states corresponding to all loop-level diagrams either satisfy the five conditions in theorem A.4.2, or are equal to $\emptyset$. Thus, lemma A.4.36 implies that all **Spek** diagrams also either satisfy these five conditions, or are equal to $\emptyset$. □

A.5 MSpek

The category **MSpek** was defined in section 4.3. We repeat the definition here for convenience.

Definition A.5.1 **MSpek** is a sub-category of **FRel**. Its objects are the same as those of **Spek**. Its morphisms are all those relations generated by composition, Cartesian product and relational converse from the generators of **Spek**, plus the following relation:

$$\perp_{\mathbf{MSpek}} : \mathrm{I} \to \mathrm{IV} :: * \sim \{1, 2, 3, 4\} \tag{A.13}$$

In this section we prove proposition A.5.2 which is repeated here for convenience:

Proposition A.5.2 All **MSpek** morphisms of type I $\rightarrow$ IV^n are subsets of IV^n containing $2^n, 2^{n+1}, \ldots, 2^{2n-1}$ or 2^{2n} n-tuples.

Proof: Clearly any **MSpek**-diagram can be obtained from a **Spek**-diagram by capping off some external legs with $\perp_{\mathbf{MSpek}}$ diagrams. Suppose for definiteness that we cap off the i^{th} leg of an n-legged **Spek**-diagram D to obtain a $(n-1)$-legged **MSpek**-diagram D'. Denoting the corresponding states by ψ' and ψ, we note from proposition A.1.8 that ψ' consists simply of the i^{th}-remnants of ψ. It is straightforward to see that each block $B \subset \psi$ gives rise to two progeny blocks B_1 and B_2: if the signature of B is $(P_1, T_1; \ldots; P_i, T_i; \ldots; P_n, T_n)$ then those of B_1 and B_2 are $(P_1, T_1; \ldots; P_i, T_i; \ldots; P_n, T_n)$ and $(P_1, T_1; \ldots; P_i', T_i; \ldots; P_n, T_n)$. Thus ψ' has 2^{m+1} blocks, each with 2^{n-m-1} tuples. There can only be duplication of blocks if ψ had contained pairs of blocks with signatures $(P_1, T_1; \ldots; P_i, T_i; \ldots; P_n, T_n)$ and $(P_1, T_1; \ldots; P_i', T_i; \ldots; P_n, T_n)$. However consideration of the effect on signatures of adding zones (propositionA.4.7), closing loops (propositions A.4.16 and A.4.21) and capping ends indicates that such pairs cannot exist in the relation corresponding to a **Spek**-diagram. Hence, ψ' has 2^n tuples, while diagram D' has $(n-1)$ legs, or alternatively ψ' has $2^{n'+1}$ tuples, while diagram D' has (n') legs. $\square$

Bibliography

[1] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium of Logic in Computer Science*, pages 415–425. IEEE Computer Science Press, 2004.

[2] H. Barnum, C. M. Caves, C. A. Fuchs, R. Josza, and B. Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett*, 76(2318), 1996.

[3] J. Barret, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Non-local correlations as an information theoretic resource. *Phys. Rev. A*, 71(022101), 2005.

[4] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195–200, 1964.

[5] C. H. Bennet and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, 1984.

[6] C. H. Bennet, G. Brassard, C. Crépeu, R. Jozsa, A. Peres, and W. K. Wooters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[7] C. H. Bennet and S. J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett*, 69(2881), 1992.

[8] D. Bohm. A suggested interpretation of the quantum theory in terms of 'hidden variables'. *Phys. Rev.*, 85:66–179, 1952.

[9] B. Coecke and R. Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. `arXiv:quant-ph/09064725`, 2009.

[10] B. Coecke and B. Edwards. Toy quantum categories. *Electronic notes in theoretical computer science*, 2008. to appear, `arXiv:0808.1037`.

[11] B. Coecke, B. Edwards, and R. Spekkens. The group theoretic origin of non-locality for qubits. Technical Report RR-09-04, OUCL, 2009.

[12] B. Coecke and E. O. Paquette. Generalized measurements and Naimarks theorem without sums. In P. Selinger, editor, *Proceedings of Quantum Programming Languages IV*, 2006.

[13] B. Coecke and D. Pavlovic. Quantum measurements without sums. In G. Chen, L. Kauffman, and S. Lamonaco, editors, *Mathematics of Quantum Computing and Technology*, pages 567–604. Taylor and Francis, 2007.

[14] B. Coecke, D. Pavlovic, and J. Vicary. A new description of orthogonal bases. Currently under review for Mathematical Structures in Computer Science. arXiv:quant-ph/0810.1037, 2008.

[15] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(062314), 2000.

[16] M. B. Elliot. *Stabilizer states and local realism*. PhD thesis, University of New Mexico, 2008. arXiv:0807.2876.

[17] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[18] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58:1131–1143, 1990.

[19] M. Hein, W. Dur, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel. Entanglement in graph states and its applications. To appear in the Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos", Varenna, Italy, July, 2005. arXiv:quant-ph/0602096v1, 2006.

[20] A. Joyal and R. Street. The geometry of tensor calculus, i. *Advances in Mathematics*, 88:55–112, 1991.

[21] G. M. Kelly and M. L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[22] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *J. Math. Mech.*, 17:59–87, 1967.

[23] S. MacLane. *Categories for the Working Mathematician*. Springer-Verlag, 1971.

[24] D. Mermin. Quantum mysteries revisited. *Am. J. Phys.*, 58:59–87, 1990.

[25] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2):436–439, 1999.

[26] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[27] D. Pavlovic. Quantum and classical structures in nondeterminstic computation. arXiv:0812.2266, 2008.

[28] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, 1994.

[29] P. Sellinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science (to appear)*, 2006.

[30] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[31] R. Spekkens. Axiomatisation through foil theories. Talk, 5 July, University of Cambridge, 2007.

[32] R. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Phys. Rev. A*, 75(032110), 2007.

[33] R. Spekkens. The power of epistemic restrictions in axiomatizing quantum theory: from trits to qutrits. Talk, 17 July, University of Oxford, 2008.

[34] J. von Neuman. *Mathematical Foundations of Quantum Mechanics*. Princeton University, 1955.

[35] W. K. Wooters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[36] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. event-ready-detectors bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, 1993.