



**Coecke, Bob and Duncan, Ross (2011) Interacting quantum observables : categorical algebra and diagrammatics. New Journal of Physics, 13 (April). ISSN 1367-2630 , <http://dx.doi.org/10.1088/1367-2630/13/4/043016>**

This version is available at <https://strathprints.strath.ac.uk/45317/>

**Strathprints** is designed to allow users to access the research output of the University of Strathclyde. Unless otherwise explicitly stated on the manuscript, Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Please check the manuscript for details of any other licences that may have been applied. You may not engage in further distribution of the material for any profitmaking activities or any commercial gain. You may freely distribute both the url (<https://strathprints.strath.ac.uk/>) and the content of this paper for research or private study, educational, or not-for-profit purposes without prior permission or charge.

Any correspondence concerning this service should be sent to the Strathprints administrator: [strathprints@strath.ac.uk](mailto:strathprints@strath.ac.uk)

## Interacting quantum observables: categorical algebra and diagrammatics

Bob Coecke<sup>1</sup> and Ross Duncan<sup>2</sup>

<sup>1</sup> Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

<sup>2</sup> Laboratoire d'Information Quantique, Université Libre de Bruxelles, Boulevard du Triomphe, B-1050, Bruxelles, Belgium

E-mail: [coecke@comlab.ox.ac.uk](mailto:coecke@comlab.ox.ac.uk) and [rduncan@ulb.ac.be](mailto:rduncan@ulb.ac.be)

*New Journal of Physics* **13** (2011) 043016 (85pp)

Received 14 April 2010

Published 14 April 2011

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/13/4/043016

**Abstract.** This paper has two tightly intertwined aims: (i) to introduce an intuitive and universal graphical calculus for multi-qubit systems, the ZX-calculus, which greatly simplifies derivations in the area of quantum computation and information. (ii) To axiomatize complementarity of quantum observables within a general framework for physical theories in terms of dagger symmetric monoidal categories. We also axiomatize phase shifts within this framework. Using the well-studied canonical correspondence between graphical calculi and dagger symmetric monoidal categories, our results provide a purely graphical formalisation of complementarity for quantum observables. Each individual observable, represented by a commutative special dagger Frobenius algebra, gives rise to an Abelian group of phase shifts, which we call the phase group. We also identify a strong form of complementarity, satisfied by the Z- and X-spin observables, which yields a scaled variant of a bialgebra.

**Contents**

<b>1. Introduction</b>	<b>3</b>
<b>2. The ZX (or green–red) graphical calculus</b>	<b>8</b>
2.1. The ZX language: networks of wires and dots	8
2.2. The ZX-equational rules	11
2.3. Interpreting the ZX-calculus in Hilbert space	14
2.4. Universality of the ZX-calculus	17
<b>3. The ZX-calculus in use</b>	<b>19</b>
3.1. Adjoints and inner products	19
3.2. Quantum circuits	20
3.3. Measurement-based quantum computing	23
<b>4. Symmetric monoidal categories and graphical reasoning</b>	<b>29</b>
4.1. Symmetric monoidal categories	30
4.2. The $\dagger$ functor	35
4.3. Diagrammatic calculus	36
4.4. Graphical reasoning	38
4.5. Correctness of graphical reasoning in ZX-calculus	39
<b>5. Vector bases and state bases of observables</b>	<b>40</b>
<b>6. Algebras and observables</b>	<b>43</b>
6.1. Monoids, comonoids and observable structures	43
6.2. Induced $\dagger$ -compact structure	48
6.3. Classical points and generalized bases	50
<b>7. Phase shifts and a generalized spider theorem</b>	<b>51</b>
7.1. A monoid structure on points	52
7.2. The decorated spider theorem	54
7.3. Unbiased points	55
7.4. The phase group	56
<b>8. Complementarity is equivalent to the Hopf law</b>	<b>58</b>
8.1. Observable structures with coinciding $\dagger$ -compact structures	58
8.2. The general case: dualizers as antipodes	60
<b>9. Closed complementary observable structures</b>	<b>61</b>
9.1. Coherence for observable structures	61
9.2. Commutation for observable structures	63
9.3. Closedness for observable structures	65
9.4. Our main theorem on pairs of closed observable structures	67
<b>10. Further group structure and the classical automorphisms</b>	<b>69</b>
<b>11. Deriving the ZX-calculus</b>	<b>71</b>
<b>12. Non-determinism, mixed states and classical data flow</b>	<b>74</b>
12.1. The CPM construction and classical concepts therein [25, 68]	75
12.2. Classicality via environment [16, 29]	77
12.3. Conditional diagrams [37]	78
<b>13. Conclusion</b>	<b>81</b>
<b>Acknowledgments</b>	<b>82</b>
<b>References</b>	<b>82</b>

## 1. Introduction

Quantum theory is arguably the single most successful scientific theory. While it is now almost a century old, many new results have been discovered by approaching quantum theory from a computational and/or information theoretic perspective, signalling the potential for a quantum information technology revolution. This approach has also led to important progress in more traditional areas of physics, for example, in condensed matter physics and statistical physics, e.g. [4], and it has provided a breath of fresh air for quantum foundations research [7, 43, 45, 72]. Most importantly, this recent wave of progress has clearly shown that much remains to be discovered concerning the quantum world, and how we reason about it.

Since von Neumann's seminal book in 1932, the *language* in which quantum theory is explained and is understood has been (and still is) that of Hilbert spaces. It is in this language that we understand key quantum mechanical concepts such as observables and complementarity thereof. While quantum information and computation (QIC) has proposed new concepts and paradigms to approach the quantum world, it has not augmented the language of quantum theory accordingly. This is in sharp contrast to the typical practice in computer science, where new perspectives and concepts are tightly intertwined with corresponding high-level language features. To make a blunt analogy, we can think of the Hilbert space formalism, where states mainly boil down to arrays of complex numbers, on the same footing as the arrays of 0's and 1's used during the Stone Age years of computer science. So one may wonder:

$$\frac{\text{high-level languages}}{b_1 b_2 \dots b_n \in \mathbb{B}^n} \simeq \frac{\text{'our aim'}}{(c_1 \ c_2 \ \dots \ c_n)^T \in \mathbb{C}^n},$$

where  $\mathbb{B}^n$  stands for strings of Booleans  $\{0, 1\}$  and  $\mathbb{C}^n$  for vectors of complex numbers.

A related issue is that of *axiomatizing* quantum theory. Despite its obvious correctness, as a language to describe quantum theory, the Hilbert space formalism seems somewhat ad hoc from a conceptual perspective. The first to acknowledge this was von Neumann himself, who for this reason denounced his own Hilbert space formalism in 1935 (see [10]), only three years after he published it. There have been many attempts to approach quantum theory in terms of mathematical structures other than Hilbert spaces [22], in the hope that this would enhance conceptual insight, but it is fair to say that none of these have provided a sufficient payoff, if any at all.

The recent advent of QIC has shed significant new light on this issue. None of the axiomatic approaches of the previous century provided an adequate mathematical vehicle for the description of compound systems, even when given the description of individual systems. On the other hand, focusing on compoundness has produced immense progress within QIC. This includes important foundational insights such as the *no-cloning theorem* [31, 77], physical phenomena such as *quantum teleportation* [8], quantum algorithms such as *polynomial time factoring* [71] and computational schemes such as *measurement-based quantum computing* [64]. Historically speaking, it was Schrödinger who emphasized compoundness as early as 1935 [67].

In this paper, we aim to catch two flies at once. We introduce a simple, intuitive, graphical high-level language, in which the atomic primitives correspond to a pair of complementary observables, and we perform an axiomatic analysis of complementarity within the very general framework of symmetric monoidal categories (SMCs). These two are related by the fact that

there is a tight correspondence between graphical languages and SMCs [47, 69], tracing back to Penrose’s work on tensor networks [61].

The diagrammatic notation is intuitive in use, but also formally rigorous (see section 4), and can lead to great simplifications in proofs. From a pragmatic point of view, the graphical language provides a compact syntax for manipulating the linear operations which are the basic elements of quantum mechanics, and it can replace more special-purpose notations such as *quantum circuits* [59] or the *measurement calculus* for measurement-based quantum computing [30], and unify these in one setting.

From an axiomatic point of view, monoidal categories are the most general mathematical framework where composing *systems* (cf the tensor product ‘ $\otimes$ ’ in the Hilbert space framework) is a fundamental action—see [17] for a more detailed discussion. Since its inception in [1], formulating quantum mechanics within monoidal categories and developing corresponding diagrammatic languages has become an active area of research.

The bottom line is: crafting a simple intuitive graphical high-level language, on the one hand, and performing an axiomatic study that places the composition of systems at the forefront, on the other hand, are in fact one and the same thing!

Our particular focus here is *complementarity* of quantum observables. In classical physics, all observables are *compatible*: they admit sharp values at the same time. In contrast, quantum observables are typically *incompatible* and cannot be assigned sharp values simultaneously. In most axiomatic approaches, incompatibility is a negative property, captured in mathematical terms by the fact that some equality fails to hold: operators that do not commute [44], probabilities that fail to obey Kolmogorov’s axioms [63], convex sets that fail to provide a simplex structure [55, 56] and lattices that do not enjoy distributivity [11, 46].

In this paper, we will take a more constructive stance and study the positive *capabilities* of a pair of maximally incompatible observables, called *complementary* or *unbiased*, and show how these capabilities are exploited in QIC. Doing so will lead to an unexpected connection between quantum computation and the area of *Hopf algebras* and *quantum groups* [13, 50], where graphical methods have also proved to be very fruitful [73].

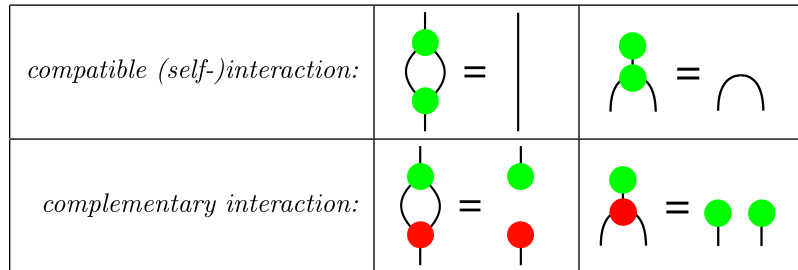
Altogether, we obtain a rich theory from rather minimal hypotheses. Many computations with elementary quantum logic gates can be carried out within this theory of *interacting observables*, as can many algorithms and protocols. To give one very basic example, the fact that the composite of two  $\wedge X$ -gates is the identity boils down to the graphical derivation:

where the dotted area is a purely graphical characterization of complementarity.

In the example above, we reasoned by *rewriting*: that is, by locally replacing some part of a diagram with a diagram equal to it. This is one of the distinctive methods of equational reasoning in graphical languages. The notion of rewriting as a formal mathematical tool has a long history in computer science (the textbooks [5] and [40] provide detailed references), and the *ZX-calculus* introduced in this paper has indeed been implemented in a software tool [32]–[34].

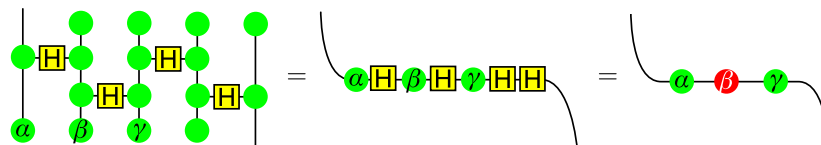
Specific physical concepts give rise to specific kinds of equations over diagrams. As the example above shows, complementary observables introduce changes in topology, characterized by disconnecting components between the red and green dots. On the other hand, in the case of compatible observables, connected components can be contracted [23, 54]. The following table

illustrates this: the green components are defined in terms of one observable, and the red ones in terms of a complementary one.



For both of the depicted interactions, complementarity yields two disconnected components, while for compatible observables connectedness is preserved. This topological distinction has very important implications for the capabilities of complementary observables in quantum informatics. The disconnectedness of the graphical form shows the absence of information flow from one component to the other, a *dynamic* counterpart to the fact that knowledge of one observable in a pair of complementary observables yields no knowledge of the other observable.

We also provide an axiomatic account of *phase shifts* relative to an observable. This leads to the mathematical concept of a *phase group*. Together, our account of complementarity and phase groups provides a universal language for reasoning about multiple two-level systems, or in modern language, qubits. For example,



is an important computation in the context of measurement-based quantum computing [65], which in Hilbert space terms would involve computations with  $32 \times 32$  matrices. This example provides a straightforward translation between quantum computational models, transforming a measurement-based configuration into a circuit.

From a mathematical perspective, we formalize observables in terms of algebras: Frobenius algebras, bialgebras, etc. These structures do not depend on having an underlying Hilbert space, or indeed any linear structure whatsoever; therefore we can study complementary observables at a much greater level of generality than the usual Hilbert space formulation of quantum mechanics. The results will apply in any ‘quantum-like’ theories that bear the necessary algebraic structures. The minimal mathematical environment to support these structures is generally a *dagger* SMC or  $\dagger$ -SMC [2, 68]. By working in an SMC, we can study the central features of quantum mechanics and quantum computation, without reference to Hilbert space at all. This research programme was initiated by Abramsky and one of the authors in [1].

In previous work, it was already established that the observables themselves correspond to certain *commutative Frobenius algebras* [27, 28]. We now explain how conceptual analysis leads to this algebraic structure, via a contrapositive of the no-cloning theorem [31, 77].

While the no-cloning theorem suggests a fundamental limitation of QIC compared to its classical counterpart, a positive reading of it reveals that quantum states may be copied *if they are known to lie in a given basis*. In other words, a quantum state may be treated as

classical data, and therefore copied freely, if it is an eigenstate of a known, non-degenerate observable. (Throughout this paper we will treat ‘orthonormal basis’ and ‘non-degenerate observable’ as synonyms, and commit abuses like ‘measuring against a basis’ and so on.) More concretely, given a finite dimensional Hilbert space  $\mathcal{H}$  with a basis  $\mathcal{A} = \{|a_i\rangle\}_i$ , the *copying operation*

$$\delta: |a_i\rangle \mapsto |a_i\rangle \otimes |a_i\rangle$$

encodes the basis  $\mathcal{A}$  as those states that it effectively copies; the no-cloning theorem guarantees that the basis vectors are the only states with this property. Note here that  $\delta$  may be realized as a unitary map on  $\mathcal{H} \otimes \mathcal{H}$  with one input fixed, for example, by  $U: |a_i\rangle \otimes |a_j\rangle \mapsto |a_i\rangle \otimes |a_{i+j}\rangle$  where the sum is taken in  $\mathbb{Z}_n$ .

Now, let  $\epsilon$  be the linear functional on  $\mathcal{H}$  defined by  $|a_i\rangle \mapsto 1$  for each  $i$ . In more conceptual terms,  $\epsilon$  uniformly *erases* the elements of the basis  $\mathcal{A}$ . Further, when  $\epsilon$  is applied to an output of  $\delta$  we get the identity map:

$$(1_{\mathcal{H}} \otimes \epsilon) \circ \delta = 1_{\mathcal{H}} = (\epsilon \otimes 1_{\mathcal{H}}) \circ \delta.$$

In algebraic terms,  $\epsilon$  is the *co-unit* for the *co-multiplication*  $\delta$ .

Together the pair  $(\delta, \epsilon)$  form a *special commutative†-Frobenius algebra* on  $\mathcal{H}$ . Previous work established the remarkable fact that *every* algebra of this kind on a finite dimensional Hilbert space arises as a pair of copying and erasing operations for some orthonormal basis [27, 28]. Since these algebras correspond precisely to non-degenerate quantum observables, we refer to them as *observable structures*. Observable structures  $(\delta, \epsilon)$  and  $(\delta', \epsilon')$  that correspond to complementary observables enjoy a special relationship: the main body of this paper is dedicated to explicating just that relationship, and a great deal of additional algebraic structure that follows.

**Structure of this paper.** This paper contains two self-contained parts, each of which could be read independently of the other:

*Part I.* Comprising sections 2 and 3, the first part is an informal presentation of a graphical calculus based on the interaction of complementary observables. Effectively we begin at the end, by presenting a calculus that demonstrates many of the key ideas of the theory, but without presenting the theory itself until part II. It also serves to familiarize the reader with graphical reasoning, a tool that we will use throughout this paper. We rely here on some familiarity with quantum computing terminology for the examples, but no other background.

Section 2 introduces the *ZX-calculus*, a graphical language and a set of equational rules that are based on the Pauli  $Z$  and  $X$  spin observables, and specially tuned for use in quantum computation. Quantum systems are represented as diagrams, and these can be rewritten according to the equations in order to prove statements about the corresponding quantum systems. This language is universal in the sense that any operation on  $n$  qubits can be expressed in it, as shown in section 2.4.

In section 3, we demonstrate a variety of applications: simulating quantum circuits and transforming measurement-based computations into equivalent circuits for example. These examples are small, but the *ZX-calculus* is appropriate for real use, and has been used to prove non-trivial results in this area [37].

*Part II.* The main body of the paper, sections 4–10 provide an axiomatic analysis of complementary observables within the general framework of †-SMC. Throughout, we will use graphical notation as much as possible.

From this point onwards, the Pauli  $Z$  and  $X$  spin observables will only be one example among all possible pairs of complementary observables. This will reveal additional properties enjoyed by the  $Z$  and  $X$  observables, as compared with other pairs of complementary observables. Also from this point onwards, Hilbert spaces are simply one particular model of the axiomatic abstract algebra, and since interpretations in other models may be useful, concepts will be introduced in full generality. For example, the observables in Spekkens' toy theory [72] are also captured by our analysis.

Section 4 reviews the necessary category-theoretic background, in particular  $\dagger$ -SMCs and their graphical notation. We rely on the work of Joyal and Street [47] and Selinger [69] to establish the validity of the graphical calculus as a rigorous mathematical syntax and not simply a sketch.

Returning briefly to the concrete Hilbert space setting, section 5 defines the notions of *state basis* and *coherent unbiased basis* for Hilbert spaces and studies their relation to quantum observables. These concepts play a key role in this paper, in abstract form, and to our knowledge have not appeared in the literature yet.

The technical core of the paper begins with section 6, which provides the definition of observable structure—also known as special commutative  $\dagger$ -Frobenius algebra—and establishes its basic properties, including the ‘spider theorem’, giving the normal form for expressions in the language of observable structures. Before arriving at the definition of complementarity, in section 7 we provide a category-theoretic account of an important related concept, namely the *phase* relative to an observable. Every observable structure gives rise to an Abelian group of phases, which behave particularly well with respect to the normal form theorem for diagrams involving observables. We refer to this result as the ‘decorated spider’ theorem.

In section 8, we characterize complementarity for observable structures. In section 9, we identify a special kind of complementary observables, which we refer to as *closed*. These include the complementary observables that are relevant to quantum computing. We moreover provide further, equivalent, characterizations of these closed complementary observables. All of these equivalent characterizations take the form of some sort of commutativity, be it either commutativity of multiplication and a comultiplication, commutativity of a multiplication and an operation, or commutativity of operations. These commutation properties present a remarkable contrast to the usual characterization of incompatibility as non-commutativity. The technical development concludes in section 10, by examining how the phase groups of complementary observables act on each other to produce ‘interference’ phenomena.

*Part III: Coda.* Section 11 returns to the beginning by demonstrating how the general theory expounded in part II produces the ZX-calculus of part I. We note which rules hold on other pairs of complementary observables, and show where the particular features of the  $Z$  and  $X$  observables appear in the calculus.

Finally, section 12 addresses the most obvious omission so far; it deals with non-determinism and classical data flow.

*About this paper.* The genesis of the current paper was an attempt to apply observable structures [23, 27]—then called *classical structures*—to a diagrammatic notation for measurement-based quantum computation [35]. An initial report on these results was first presented at the ICALP conference in 2008 [18], albeit under severe space restrictions. During the intervening period the theory was under active development in Oxford, and several papers have appeared making use of the key ideas and applying them in various settings: in



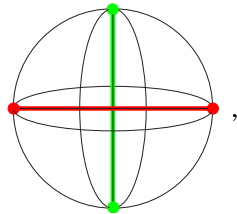
measurement-based quantum computation [36, 37], in the study of Spekkens' toy theory and non-locality [19, 20], quantum protocols [29], complementarity in the category of relations [19, 41, 60], among others. This paper is the first complete presentation of our categorical treatment of complementary observables, and it corrects several errors in the earlier paper.

## 2. The ZX (or green–red) graphical calculus

The state space of the elementary quantum computational unit, the *qubit*, is denoted by  $\mathcal{Q} := \mathbb{C}^2$ . The vectors of the *computational basis* or *Z-basis* are written as  $|0\rangle, |1\rangle$ , while those of the *X-basis* are written as

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

On the Bloch sphere these bases can be represented as follows:



where the green dots represent the elements of the *X-basis* and the red dots represent those of the *Z-basis*.

These bases consist of the eigenvectors of the Pauli spin matrices,

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (1)$$

and correspond to the possible outcomes upon measuring the spin of the electron along the *Z*- and *X*-axes, respectively. Our interest in these particular spins stems from the fact that they are the simplest example of *complementary observables*.

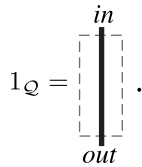
In this section, we will present a graphical calculus, specific to the *Z*- and *X*-spin observables, which is a special case of the general theory that we develop later in this paper. As well as demonstrating the main features of the full theory, this simplified calculus is sufficiently powerful to carry out many calculations useful in the context of quantum computation, as the examples in section 3 will demonstrate.

This framework refers exclusively to the mathematics underlying quantum computation and not to any details of how the operations are implemented, which makes it ideal for unifying various approaches to quantum computation. For example, we can demonstrate equivalence between different quantum computational models.

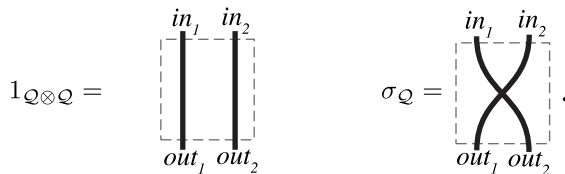
### 2.1. The ZX language: networks of wires and dots

The ZX-calculus consists of components joined by wires, similar to electronic circuit diagrams or flow charts. The simplest non-trivial diagram in the language is simply a wire running from

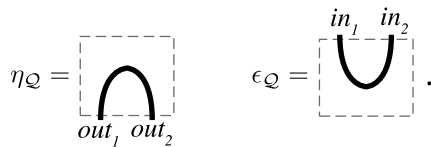
top to bottom:



We think of diagrams as being enclosed in a box with a certain number of points through which wires enter and leave; that is, each diagram has a fixed *interface*. Exactly one wire must be present at each point of the interface, and we must distinguish which wire is connected to which point. Indeed, this is the only difference between the two diagrams below.



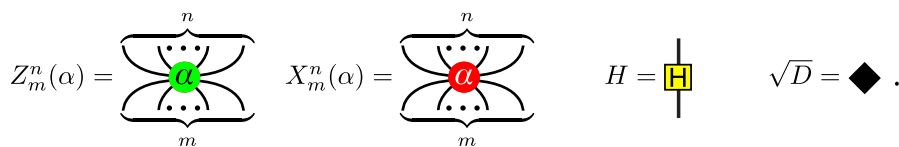
It is not important whether crossing wires pass over or under (i.e. we are in a symmetric setting, not a *braided* one [48]). Wires may bend, linking two outputs to form a cap, or two inputs to form a cup.



From here on, the inputs and outputs will not be named, and are distinguished simply by their ordering from left to right. We write  $\mathcal{D}: m \rightarrow n$  to indicate that the diagram  $\mathcal{D}$  has  $m$  inputs and  $n$  outputs.

Aside from wires, the ZX-calculus contains four kinds of components:

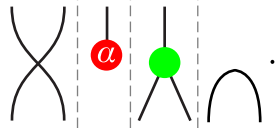
- $Z$  vertices (green dots), labelled by an angle  $\alpha \in [0, 2\pi)$ , called the *phase*. These can have any number of inputs or outputs (including none).
- $X$  vertices (red dots), labelled by a phase. These too can have any number of inputs or outputs (including none).
- $H$  vertices (yellow squares). These must have exactly one input and one output.
- $\sqrt{D}$  vertices (black diamonds). These may not have any inputs or outputs.



We refer to the  $Z$  and  $X$  vertices as ‘spiders’, and make the convention that if  $\alpha = 0$  the angle is omitted.

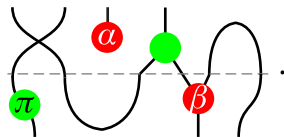
Diagrams are built from these generators—straight, crossing and bending wires and  $Z$ ,  $X$ ,  $H$  and  $\sqrt{D}$  vertices—in two manners.

- Placing them side-by-side:



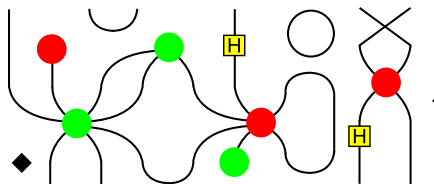
*Notation:* Given  $\mathfrak{D}: m \rightarrow n$  and  $\mathfrak{D}': m' \rightarrow n'$  their *tensor product* is denoted by  $\mathfrak{D} \otimes \mathfrak{D}': m + m' \rightarrow n + n'$ .

- Connecting outputs to inputs:



*Notation:* Given  $\mathfrak{D}_1: m \rightarrow n$  and  $\mathfrak{D}_2: n \rightarrow k$  their *composition* is denoted by  $\mathfrak{D}_2 \circ \mathfrak{D}_1: m \rightarrow k$ .

Therefore, the terms of graphical ZX-language are networks of vertices of each type, straight, crossing and bent wires:



In such a network, there can be no ‘loose wires’: every wire must terminate at a vertex, or else be an input or output.

Important examples are those spiders with two inputs and one output (cf a binary operation), with no input and one output (cf initiation of a value) which we will call a *point*, with one input and two outputs (cf copying) and with one input and no output (cf erasing):



As we will see shortly, these unlabelled spiders play a special role in the calculus, as do those labelled by  $\pi$ .

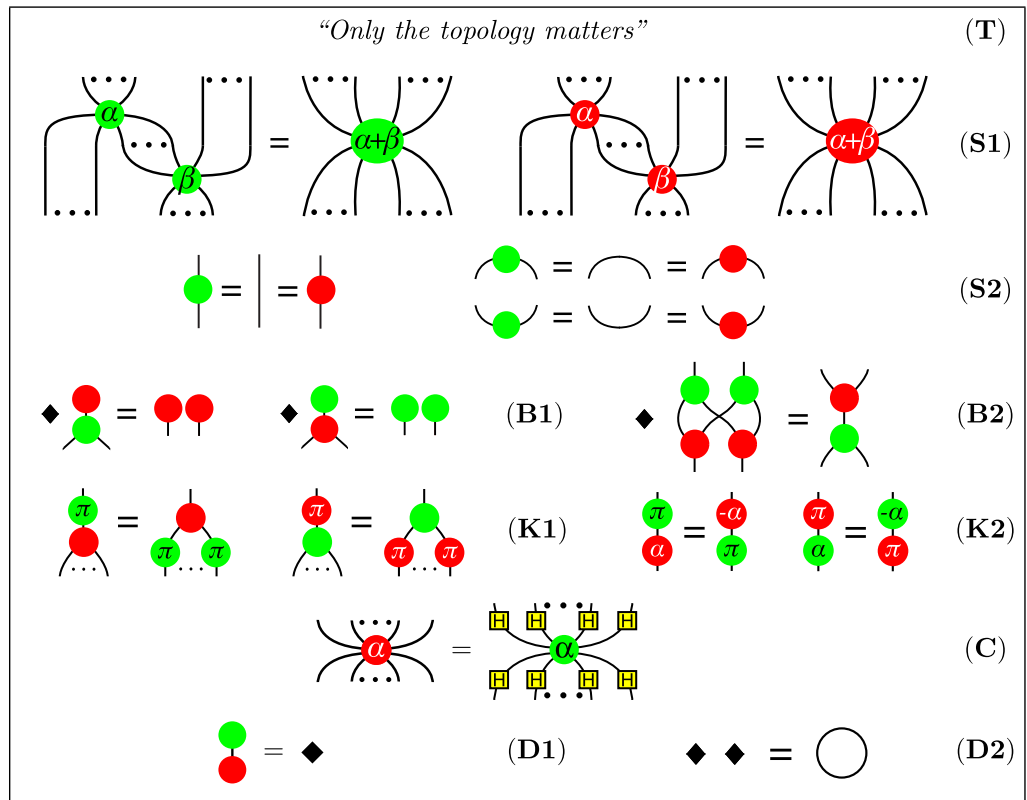


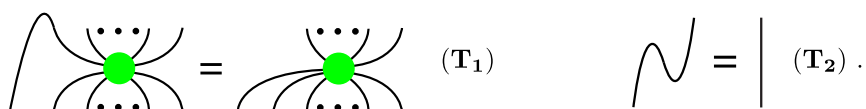
Figure 1. Rules for the ZX-calculus

2.2. The ZX-equational rules

In addition to the rules for constructing diagrams, the calculus consists of a set of equations that specify how one diagram may be transformed into another. These rules are presented in figure 1. We now expand on these rules and give some examples of their use.

2.2.1. The T-rule. The informally stated T-rule will be made more precise in sections 4.3–4.5. For practical purposes, the intuitive reading of ‘only the topology matters’ suffices: the wires of the diagram may be arbitrarily stretched, bent, twisted, tied in knots, etc, without altering the meaning of the diagram, provided the connections are maintained. More precisely, after identifying (e.g. by enumerating) the inputs and the outputs, any topological deformation of the internal structure of the network yields a network that is equal to the given one.

Two important examples of such ‘homotopic rewrites’ are



In fact, these two rules can also be seen as consequences of the S-rules, when introducing a green dot on the caps and cups as in (S2); see example 2.4 below. The reason for considering them within the T-rule will become clear in section 4.5.

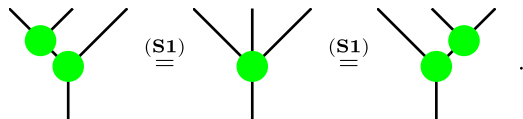
**Remark 2.1.** *Since wires can be stretched without consequence, adding a straight length of wire to the input or output of the diagram has strictly no effect. Hence bundles of straight wires act as identity elements in the algebra of diagrams.*

**Remark 2.2.** *While the slogan says ‘only the topology matters’, this does not imply that the topology is always preserved. The other rules may change the topology of the diagram in various ways, for example to remove loops or to disconnect previously connected vertices.*

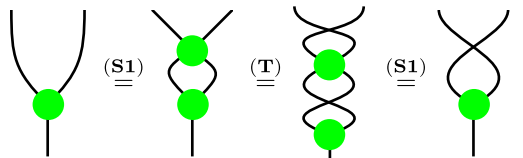
2.2.2. *The S-rules.* The ‘spider’ rules govern how dots of the same colour interact. Rule (S1) states that connected dots of the same colour can be merged, summing the phases; conversely, a dot can be ‘decomposed’ along one or more connecting wires. Note that the number of connecting wires is irrelevant.

The equations (S2) specify when spiders are trivial: dots of degree 2 with phase  $\alpha = 0$  can be removed, or conversely, introduced.

**Example 2.3.** *If we view the dot  $Z_1^2: 2 \rightarrow 1$  as a binary operation, (S1) tells us that it is associative:*

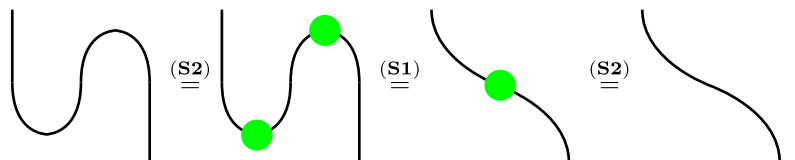


*Less obviously, (S1) implies that this operation is commutative:*



*We leave the reader the (easy!) exercise of showing that  $Z_1^0$  is a unit for this operation, and hence that we have a commutative monoid<sup>3</sup>.*

**Example 2.4.** *The (T<sub>2</sub>) rule can be derived using the S-rules:*



*The (T<sub>1</sub>) rule is derived similarly.*

Mathematically, the two S-rules state that each family of coloured dots forms a *special commutative dagger-Frobenius algebra*, equipped with a *phase group*. This will be elaborated upon in sections 6 and 7.

<sup>3</sup> That is, a set with a commutative associative unital operation.

2.2.3. *The B-rules.* The **B1**-rule can be read loosely as ‘green copies red points’ and ‘red copies green points’, in both cases ‘up to a diamond’.

The **B2**-rule is a powerful commutation principle, and generates a whole family of equations, allowing alternating cycles of red and green dots to be replaced with simpler graphs; see [36].

**Example 2.5.** *An important equation derivable from the B-rules is the following:*

(B').

*This equation is obtained as follows:*

*Note that the step labelled (B1) in fact applies a version of that rule deformed by (T), without altering the topology. We could do this more explicitly using the  $T_1$  and  $T_2$  examples as follows:*

Rules **(B')** and **(B2)** are known informally as the *Hopf law* and the *bialgebra law*. Together, the **B**-rules state that the interactions of different coloured spiders produce a structure we call a *scaled bialgebra*, which differs from a bialgebra only by a normalizing factor. The fact that these structures naturally arise whenever we have complementary observables is one of the main insights of this paper, and will be developed further in section 8.

2.2.4. *The K-rules.* These rules are concerned with special properties of spiders with phase  $\alpha = \pi$ . Rule **(K1)** states that dots labelled by  $\pi$  commute with spiders of the other colour, i.e.  $X_1^1(\pi)$  is a homomorphism of the comultiplication  $Z_2^1(0)$ , and vice versa.

**Example 2.6.** *Thanks to rule (K1), points with phase  $\pi$  can also be copied just like points with phase zero:*

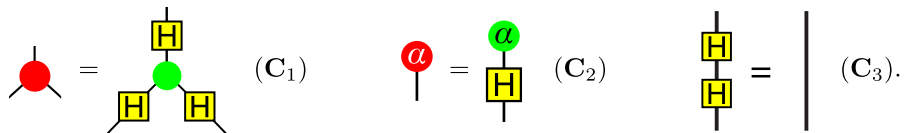
Since the points labelled by  $\pi$  or 0 can be copied, we call these *classical points*; then  $Z_1^1(\pi)$  and  $X_1^1(\pi)$  are called *classical maps*.<sup>4</sup> (Of course, **K** stands for ‘klassical’.) In the next section, we will see that  $Z_1^1(\pi)$  and  $X_1^1(\pi)$  are interpreted by the familiar Z and X gates, respectively.

Rule (**K2**) states that dots labelled by  $\pi$  invert the phase of dots of the other colour.

**Example 2.7.** By rules (**S1**) and (**S2**), the degree 2 spiders  $Z_1^1(\alpha)$  form an Abelian group, and by (**K2**), conjugation by  $X_1^1(\pi)$ —note here that  $X_1^1(\pi)$  is self-inverse since  $\pi + \pi = 0$ —sends each element to its inverse.

2.2.5. *The C-rule.* This rule allows the  $H$  vertex to function as an explicit colour changing operation that transforms ‘green structures’ into ‘red structures’ and vice versa. In the next section, we will see that the  $H$  vertex is interpreted by the familiar Hadamard gate, exchanging the  $X$  and  $Z$  bases.

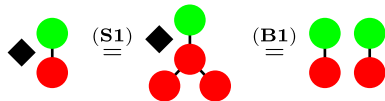
**Example 2.8.** Some special cases of this rule are



Note that (**C3**) asserts that  $H$  is self-inverse. The **C**-rule effectively allows  $H$  vertices to commute with coloured dots, changing their colour in the process.

2.2.6. *The D-rules.* The (**D2**) rule states that two black diamonds are equal to a loop of wire, itself the result of composing a cup and a cap. We will see in the next section that the loop represents the dimension of the underlying Hilbert space, and spacial juxtaposition is a form of multiplication, justifying the name  $\sqrt{D}$  for the diamond.

The (**D1**) rule ‘almost follows’ from the other rules:



which would yield the desired result if  $\bullet$  could be cancelled.

### 2.3. Interpreting the ZX-calculus in Hilbert space

Given a diagram  $\mathcal{D}$  with  $n$  inputs and  $m$  outputs, we construct a corresponding linear map  $D: \mathcal{Q}^n \rightarrow \mathcal{Q}^m$  as follows.

**Definition 2.9** (interpretation of generators). *If  $\mathcal{D}$  consists of just a single generator—that is, one of  $1_{\mathcal{Q}}$ ,  $\sigma_{\mathcal{Q}}$ ,  $\eta_{\mathcal{Q}}$ ,  $\epsilon_{\mathcal{Q}}$ ,  $Z_m^n(\alpha)$ ,  $X_m^n(\alpha)$ ,  $H$ , or  $\sqrt{D}$ —then its corresponding linear map is as shown below:*

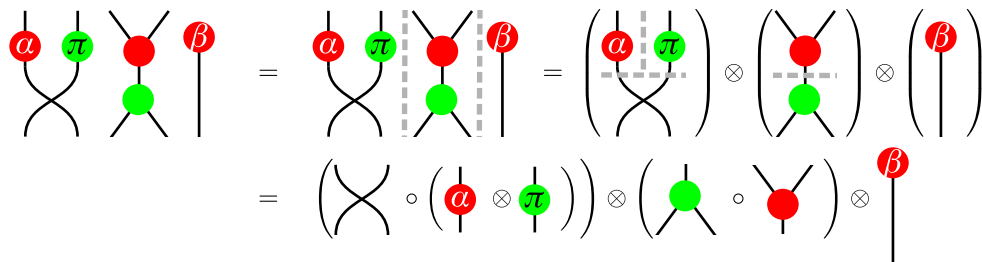
<sup>4</sup> That is, classical relative to a particular observable structure; these classical maps then act as a permutation on the classical points of the observable structure [25].





The order in which we divide the diagram into pieces does not matter to the final result, so long as the ‘cuts’ do not pass through any vertices or any points where wires cross or any points of inflection of a wire—more accurately: just those inflection points where the gradient of the wire changes sign. (These last two may be thought of as the ‘vertices’ defining  $\sigma_Q$ , and  $\eta_Q$  and  $\epsilon_Q$ , respectively.)

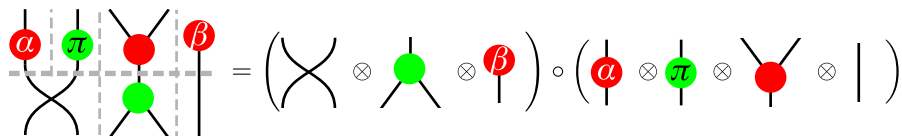
**Example 2.13.** *The following diagram can be divided up as follows:*



giving the linear map

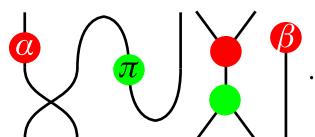
$$D = \left( \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \left( e^{-i(\alpha/2)} \begin{pmatrix} \cos \frac{\alpha}{2} & i \sin \frac{\alpha}{2} \\ i \sin \frac{\alpha}{2} & \cos \frac{\alpha}{2} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right) \right. \\ \left. \otimes \frac{1}{\sqrt{2}} \left( \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \otimes e^{-i(\beta/2)} \begin{pmatrix} i \sin \frac{\beta}{2} \\ \cos \frac{\beta}{2} \end{pmatrix} \right).$$

Unlike the diagram, the resulting matrix is rather large ( $16 \times 32$ ), so it is not shown here. Any other factorization of the diagram, for example,



produces the same interpretation.

**Example 2.14.** *According to the T-rule, the diagram of example 2.13 above is equivalent to the one shown below:*



As one might hope, this gives the same interpretation.

**Remark 2.15.** A linear map  $f: \mathbb{C} \rightarrow \mathbb{C}$  is completely determined by the value  $f(1)$ . For this reason, and since  $\mathcal{Q}^0 = \mathbb{C}$ , the Hilbert space interpretation of a diagram with no inputs or outputs—a map from  $\mathbb{C}$  to itself—is simply a complex number.

**Proposition 2.16** (Soundness). *If diagrams  $\mathfrak{D}_1$  and  $\mathfrak{D}_2$  are equal according to the equational rules of the ZX-calculus, then  $D_1 = D_2$ .*

This proposition can largely be verified by computing the maps corresponding to the left and right sides of each of the equational rules given in figure 1, and observing that they are equal. However, to show that the **T**-rule is correct, different techniques are required. We will return to this point, and the (non)-issue of the factorization order, in section 4.3.

The converse of proposition 2.16 is false: there exist diagrams  $\mathfrak{D}_1$  and  $\mathfrak{D}_2$  that represent the same linear map but which are not equal by the rules of the ZX-calculus. For example, the following diagrams are not equivalent in the calculus:

but their interpretation as linear maps is the Euler-angle decomposition,

$$H = Z_1^1\left(\frac{\pi}{2}\right) \circ X_1^1\left(\frac{\pi}{2}\right) \circ Z_1^1\left(-\frac{\pi}{2}\right).$$

This equation is equivalent to Van den Nest's theorem on local complementation of graph states [75], as shown elsewhere by Perdrix and one of the present authors [36].

We remark upon this fact for two reasons: firstly, as warning that not every true fact about Hilbert space quantum mechanics can be derived using the ZX-calculus, although a great many equations used in quantum information processing can be. Secondly, since the equational theory of the ZX-calculus is strictly weaker than that of Hilbert spaces, it is more general. Therefore, there are models of the calculus which are distinct from the usual Hilbert space interpretation of quantum mechanics. All such models contain a large fragment of quantum mechanics—viewed as an equational theory—but facts like Van den Nest's theorem need not hold.

**Remark 2.17.** *The points in the calculus are not normalized. This is required for reasons of simplicity; if we were to normalize  $\sigma_{\mathcal{Q}}$  and  $\eta_{\mathcal{Q}}$ , then the **(TI)** rule would require additional scalar multipliers, and hence so would the **(SI)** rule, and so on.*

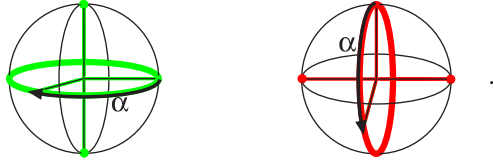
#### 2.4. Universality of the ZX-calculus

We claim that we now have enough expressive power to write down any arbitrary linear map from  $n$  qubits to  $m$  qubits. The green and red phases, respectively,

$$\begin{array}{c} \bullet \\ | \\ \alpha \end{array} = Z_1^1(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \quad (2)$$

$$\begin{array}{c} \bullet \\ | \\ \alpha \end{array} = X_1^1(\alpha) = e^{-i\alpha/2} \begin{pmatrix} \cos \frac{\alpha}{2} & i \sin \frac{\alpha}{2} \\ i \sin \frac{\alpha}{2} & \cos \frac{\alpha}{2} \end{pmatrix} \quad (3)$$

correspond to rotations of angle  $\alpha$ , respectively, around the Z- and X-axis on the Bloch sphere:



Combining both the ‘green’ and the ‘red’ phases allows us to write down any arbitrary one-qubit unitary in terms of its Euler-angle decompositions on the Bloch sphere:

$$\begin{array}{c} \alpha \\ \beta \\ \gamma \end{array} = Z_1^1(\gamma) \circ X_1^1(\beta) \circ Z_1^1(\alpha). \tag{4}$$

The controlled-NOT gate is defined by

$$\begin{array}{c} \bullet \\ \bullet \end{array} \text{---} \begin{array}{c} \bullet \\ \bullet \end{array} := \begin{array}{c} \bullet \\ \bullet \end{array} \text{---} \begin{array}{c} \bullet \\ \bullet \end{array} \stackrel{T_1 T_1}{=} \begin{array}{c} \bullet \\ \bullet \end{array} \text{---} \begin{array}{c} \bullet \\ \bullet \end{array} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \wedge X. \tag{5}$$

Standard results in quantum computing [59] state that  $\wedge X$  gates and arbitrary one-qubit unitaries suffice to construct any  $n$ -qubit unitary map. As equations (4) and (5) show, the ZX-calculus contains this universal gate set, and hence can represent any  $n$ -qubit unitary map. Arbitrary  $n$ -qubit states can therefore be represented as the image of any  $n$ -qubit state—for example  $\begin{array}{c} \bullet \\ \dots \\ \bullet \end{array}$ —under a well-chosen unitary. Finally,  $\cup = \langle 00| + \langle 11|$  allows us to obtain any arbitrary linear map  $f$  from  $n$  qubits to  $m$  qubits from some  $n + m$  qubit state  $|\Psi\rangle$ , by relying on the diagrammatic incarnation of map–state duality [1]:

$$\begin{array}{c} \overbrace{\begin{array}{c} \bullet \\ \dots \\ \bullet \end{array}}^n \\ \text{---} \\ \text{---} \\ \text{---} \\ \underbrace{\begin{array}{c} \bullet \\ \dots \\ \bullet \end{array}}_m \end{array} = \begin{array}{c} \Psi \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array}. \tag{6}$$

Summarizing all this:

**Proposition 2.18.** *Let  $A: \mathcal{Q}^n \rightarrow \mathcal{Q}^m$  be a linear map; then there exists a diagram  $\mathfrak{A}$  in the ZX-calculus whose Hilbert space interpretation is  $A$ .*

**Remark 2.19.** *Since the converse to proposition 2.16 does not hold, there is no reason why the diagram  $\mathfrak{A}$  should be unique. There could be many inequivalent diagrams all of which denote the same linear map.*

### 3. The ZX-calculus in use

#### 3.1. Adjoints and inner products

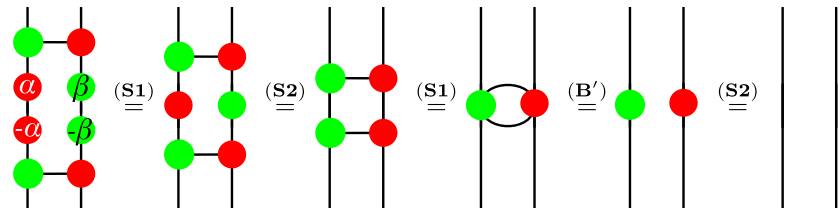
**Definition 3.1.** Let  $\mathcal{D}: m \rightarrow n$  be a diagram; then its adjoint,  $\mathcal{D}^\dagger: n \rightarrow m$ , is a diagram constructed by reflecting  $\mathcal{D}$  in the horizontal axis, and negating all the angles that occur in  $\mathcal{D}$ .

A diagram  $\mathcal{D}$  is called *self-adjoint* if  $\mathcal{D} = \mathcal{D}^\dagger$ , and *unitary* if  $\mathcal{D} \circ \mathcal{D}^\dagger = 1_{\mathcal{Q}^{\otimes n}}$  and  $\mathcal{D}^\dagger \circ \mathcal{D} = 1_{\mathcal{Q}^{\otimes m}}$ .

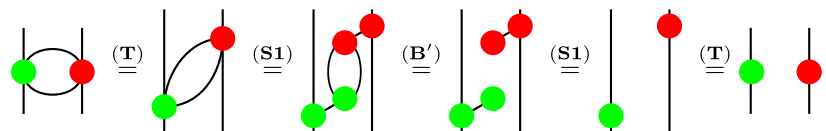
**Example 3.2.** Given the diagram  $\mathcal{D}$ , we form its adjoint  $\mathcal{D}^\dagger$  as shown:



We claim that  $\mathcal{D}$  is unitary. Half of the required proof is shown below.



The ‘horizontal application’ of the  $B'$ -rule can be decomposed as follows:



from which it follows that pairs of wires between green and red dots can be eliminated. It remains to be shown that  $\mathcal{D} \circ \mathcal{D}^\dagger = 1_{\mathcal{Q}^2}$ .

The following is self-evident:

**Proposition 3.3.** Let  $\mathcal{D}$  be some diagram. Then (i)  $\mathcal{D}^{\dagger\dagger} = \mathcal{D}$ ; (ii) if  $\mathcal{D} = \mathcal{A} \circ \mathcal{B}$ , then  $\mathcal{D}^\dagger = \mathcal{B}^\dagger \circ \mathcal{A}^\dagger$ ; and (iii) if  $\mathcal{D} = \mathcal{A} \otimes \mathcal{B}$ , then  $\mathcal{D}^\dagger = \mathcal{A}^\dagger \otimes \mathcal{B}^\dagger$ .

**Proposition 3.4.** If  $D: m \rightarrow n$  denotes the linear map  $D: \mathcal{Q}^m \rightarrow \mathcal{Q}^n$ , then the adjoint diagram  $\mathcal{D}^\dagger$  denotes  $D^\dagger$ , the usual linear algebraic adjoint of  $D$ .

**Corollary 3.5.** If a diagram is self-adjoint or unitary, so is its corresponding linear map.

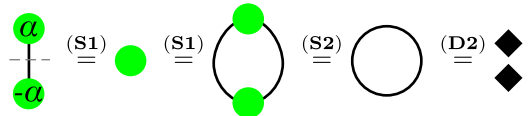
Recall that any diagram  $\mathcal{D}: 0 \rightarrow n$  has a (possibly unnormalized)  $n$ -qubit state as its Hilbert space interpretation; such diagrams therefore correspond to kets  $|\mathcal{D}\rangle$  in Dirac notation. Since Dirac’s bra is the adjoint of a ket, we now see how to define the inner product of two diagrams.

Given  $\mathfrak{A}, \mathfrak{B}: 0 \rightarrow n$  we have

$$\langle \mathfrak{A} | \mathfrak{B} \rangle = \mathfrak{A}^\dagger \circ \mathfrak{B}.$$

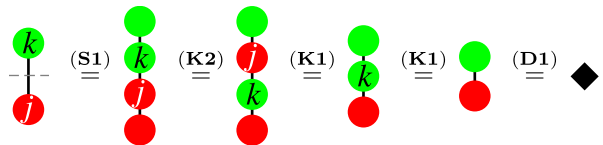
The resulting diagram  $(\mathfrak{A}^\dagger \circ \mathfrak{B})$  has no inputs or outputs; hence by remark 2.15, it denotes complex number, as required.

**Example 3.6.** We can compute the inner product of  $Z_1^0(\alpha)$  with itself.



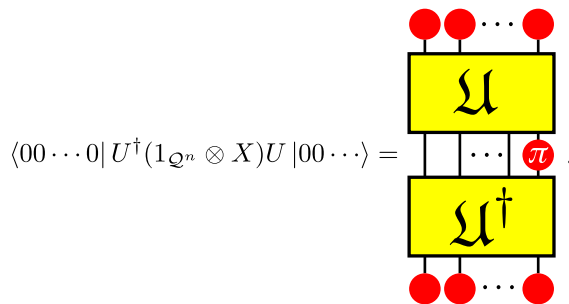
The result is 2 because the ‘states’ are not normalized.

**Example 3.7.** Let  $j, k \in \{0, \pi\}$ . We compute the inner product of  $Z_1^0(k)$  and  $X_1^0(j)$ .



Since the result is independent of  $j$  and  $k$ , this calculation shows that the  $X$  and  $Z$  bases are mutually unbiased.

**Example 3.8.** Suppose that  $\mathfrak{U}$  is a diagram encoding some complicated unitary operation  $U$ , acting on  $n + 1$  qubits. Suppose its input is  $|00 \dots 0\rangle$ : what is the amplitude for observing the output  $|1\rangle$  at its last output? We need to compute:

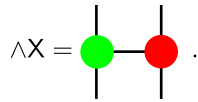


When  $\mathfrak{U}$  is presented using the generators of the ZX-calculus, a great simplification is (usually) possible, making this expression (usually) easy to compute.

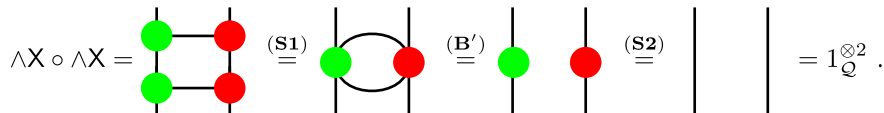
### 3.2. Quantum circuits

As we have already seen in section 2.4, the ZX-calculus can represent the basic gates used in quantum circuits. The rules of the calculus can give short graphical proofs of many circuit identities.

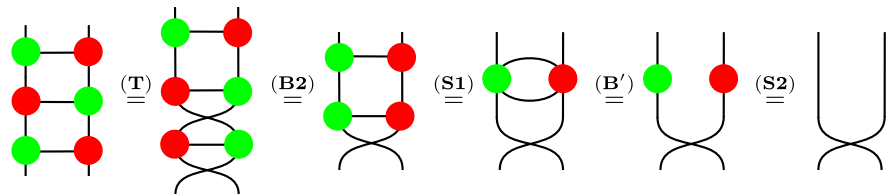
3.2.1. *The  $\wedge X$  gate.* We have already seen the controlled-NOT gate:



It is manifestly self-adjoint. We can prove that it is also unitary:

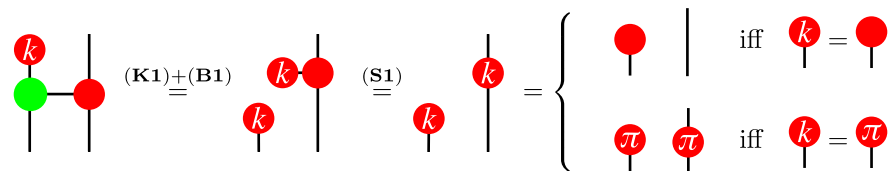


An elementary exercise is to show that a sequence of three  $\wedge X$  gates can be used to swap two qubits. A graphical proof of this fact is given below.



While this is a well-known property for  $\wedge X$ , our proof holds in much greater generality than qubits, since as we will see in the remainder of this paper, the graphical calculus applies in much greater generality. This example relies on the bialgebra law **(B2)**, which is a stronger principle than the Hopf law **(B')** used in the previous example. The relationship between these two laws will be spelled out in section 9.

In section 2.4, the  $\wedge X$  gate was introduced by checking that its diagram denoted the correct linear map. However, we can describe  $\wedge X$  by the following ‘behavioural specification’: *when the control input is  $|0\rangle$ , the target qubit is left unchanged; when the control qubit is  $|1\rangle$ , the target qubit is flipped.* Letting  $\uparrow^k$  represent one of the two red classical points, that is, either  $\uparrow^k = |0\rangle$  or  $\uparrow^\pi = |1\rangle$ , we can supply a qubit to the control input (the left input, connected to the green dot), and obtain the following proof:

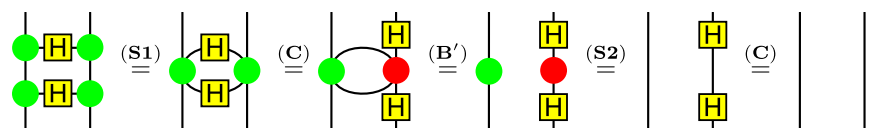


Note that in each case the control qubit passes through the gate unchanged, while the target input is either the identity or the Pauli X, depending on the value of the control qubit, thus meeting the specification. Further, the colour symmetry of this proof demonstrates that if we operate in the Z-basis (i.e.  $|+\rangle = \uparrow^{\text{green}}$  and  $|-\rangle = \uparrow^{\text{red}}$ ), the roles of left and right are exchanged.

3.2.2. *The  $\wedge Z$  gate.* Since  $Z = HXH$ , we can obtain the  $\wedge Z$  gate from the  $\wedge X$  gate by conjugating the target qubit with  $H$  gates, as shown below:

$$\wedge Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \text{Circuit with } \wedge X \text{ and } H \text{ gates} = \text{Circuit with } \wedge X \text{ and } H \text{ gates}.$$

We can immediately read off two properties of this gate from its graphical representation: it is self-adjoint, and it is symmetric in its inputs. It is also unitary:

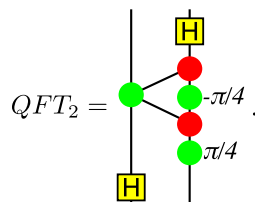


3.2.3. *The quantum Fourier transform.* Lying at the centre of many quantum algorithms—including Shor’s famous factoring algorithm [71]—the quantum Fourier transform is one of the most important quantum processes. The equations of the diagrammatic calculus are strong enough to simulate it.

To write down the required circuit, we must realize a controlled phase gate, where the phase is an arbitrary angle  $\alpha$ ; this is shown below—the control qubit is on the left. (One can prove the correctness of this diagram using a behavioural description in a similar fashion to the treatment of the  $\wedge X$  in section 3.2.1.)

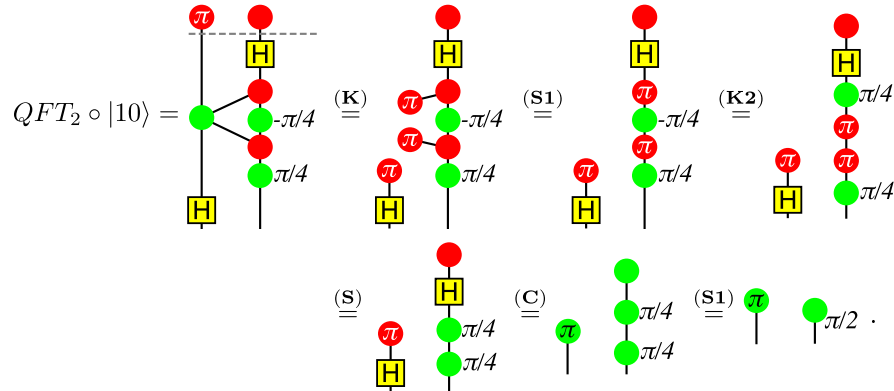
$$\wedge Z_\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} = \text{Circuit with } \wedge X \text{ and } \text{phase gates } \alpha/2, -\alpha/2.$$

The only gates that are required to construct the circuit implementing the quantum Fourier transform are the Hadamard and the  $\wedge Z_\alpha$ —see for example [59]. The circuit for the two-qubit QFT is shown below.



How can we simulate this circuit? First, we choose an input state, in this case  $|10\rangle = \uparrow \downarrow$ ; then we simply concatenate the input to the circuit, and begin rewriting according to the equations

of the theory, as shown below.



The final diagram in the sequence is simply the tensor product  $(|0\rangle - |1\rangle) \otimes (|0\rangle + i|1\rangle)$ , which is indeed the desired result. In passing we remark on another feature of the graphical language: since the last diagram is a disconnected graph, it represents a separable quantum state.

### 3.3. Measurement-based quantum computing

Measurement-based quantum computation [49] uses the state-changing effect of quantum measurements to carry out the computation, typically propagating these changes through entangled states. The simplest example is the teleportation protocol [8], which can be viewed as the identity function computed via a Bell state. A more powerful model is Raussendorf and Briegel's one-way quantum computer [64, 65], which provides a computationally universal model almost entirely based on single-qubit measurements acting on a large cluster state.

The graphical notation of the ZX-calculus is ideal for representing these entangled states, and its equations accurately capture the changes in these states induced by measuring their constituent parts.

**Remark 3.9.** *The ZX-calculus, as presented in this section, cannot represent the non-deterministic behaviour of measurements. Rather, we replace measurements by projections onto some particular outcome. One could view this as post-selection, but it would be more accurate to understand that each diagram represents one particular run of an experiment, and the particular outcome that was measured, rather than averaging over all possible runs. The restriction to pure states is not an intrinsic limitation of this approach. It is a deliberate choice, made in order to simplify the presentation of the calculus. The formal apparatus used here was introduced in [27] to represent the classical control structure and the branching behaviour of quantum measurements. In section 12, we present three extensions to the calculus to handle non-determinism and mixedness.*

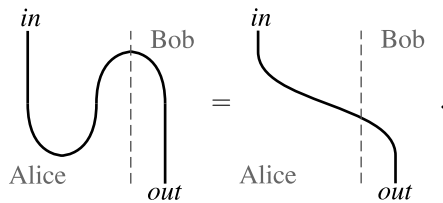
**3.3.1. The teleportation protocol.** The teleportation protocol [8] consists of two main components: the preparation of the Bell state and the Bell basis measurement. As described



in section 2.3, the (unnormalized) Bell state is represented by a cap, and its corresponding projection by a cup:

$$|00\rangle + |11\rangle = \text{cap}, \quad \langle 00| + \langle 11| = \text{cup}.$$

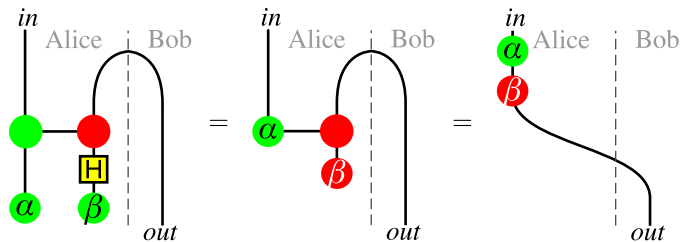
Combining these two elements, we obtain an almost trivial proof of the correctness of teleportation, in the case where Alice observes  $|00\rangle + |11\rangle$ .



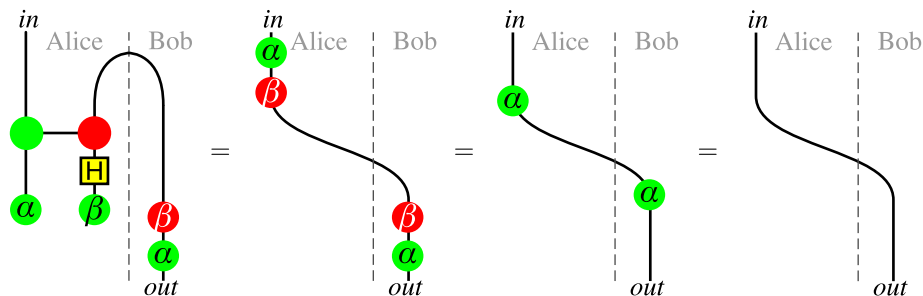
The role of classical communication is hidden in this picture, but it is revealed by a more detailed look at the Bell basis measurement. Let  $\alpha, \beta \in \{0, \pi\}$ . Ranging over the four possible  $(\alpha, \beta)$  pairs in the diagram below gives the four possible outcomes of a Bell basis measurement:

$$\{ \langle \Psi_+ |, \langle \Psi_- |, \langle \Phi_+ |, \langle \Phi_- | \} = \left\{ \begin{array}{c} \text{circuit with } \alpha, \beta \text{ and } \text{H} \text{ gate} \\ | \alpha, \beta \in \{0, \pi\} \end{array} \right\}.$$

(Note that the boxed part of the diagram is simply the circuit that rotates the Bell basis onto the X-basis.) This description of the protocol displays the Pauli errors that are introduced if Alice observes the other possible outcomes.



From this we can derive a complete description of the protocol, and show, including Bob's corrections, which are classically correlated to Alice's observations.



The first equation is the preceding derivation collapsed into one step, while the last two equations use the spider rules and the fact that  $2\alpha = 2\beta = 0$ .

3.3.2. *The state transfer protocol.* This protocol was introduced by Pedrix [62] to reduce the resources required for measurement-based quantum computing. The core of the protocol is a measurement which projects onto a two-dimensional (2D) eigenspace:

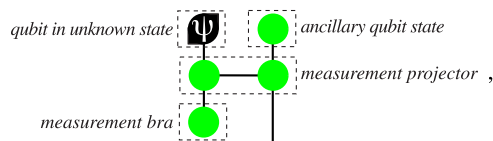
$$\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \stackrel{\text{S}}{=} \begin{array}{c} \diagup \bullet \diagdown \\ \diagdown \bullet \diagup \end{array} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = P_{Z \otimes Z}. \tag{7}$$

It is easily seen that  $P_{Z \otimes Z}$  is self-adjoint and idempotent:

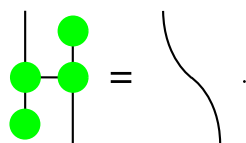
$$P_{Z \otimes Z} \circ P_{Z \otimes Z} = \begin{array}{c} \bullet \quad \bullet \\ | \quad | \\ \bullet \quad \bullet \\ | \quad | \\ \bullet \quad \bullet \end{array} \stackrel{\text{S}}{=} \begin{array}{c} \diagup \bullet \diagdown \\ \diagdown \bullet \diagup \end{array} \stackrel{\text{S}}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} = P_{Z \otimes Z}, \tag{8}$$

and hence a projector.

Consider now a protocol, which initially assumes two qubits, one in an unknown state  $|\Psi\rangle = |\psi\rangle$  and one in the state  $|+\rangle$ . We want to transfer  $|\psi\rangle$  from the first qubit to the second, and this can be done by means of two projections:



since by application of the S-rule we have



The protocol can be extended by performing the second, single-qubit measurement in the phase-shifted basis  $|0\rangle \pm e^{i\alpha}|1\rangle$ .

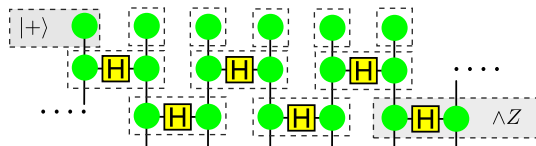
$$\begin{array}{c} \bullet \\ | \\ \bullet \quad \bullet \\ | \quad | \\ \bullet \quad \bullet \\ | \quad | \\ \bullet \quad \bullet \end{array} \stackrel{\text{(S)}}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

The diagram shows two vertical lines with green circles at the top, connected by a horizontal line. The bottom-left green circle is enclosed in a dashed box labeled 'measurement bra with phase'. This is equal to a single vertical line with a green circle at the top, labeled with a green  $\alpha$ .

This minor change allows the protocol to apply an arbitrary Z-rotation to its input; the protocol can be modified in the obvious way to perform an X-rotation, and hence any single-qubit unitary.

3.3.3. *Multipartite states.* In our graphical language, a quantum state is nothing more than a diagram with no inputs; the outputs correspond to the individual qubits making up the state. The interior of the diagram—i.e. its graph structure—describes how these qubits are related. This notation is ideal for representing large entangled states.

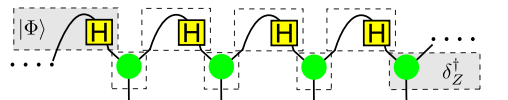
Cluster states, which are used in measurement-based quantum computing [65], can be prepared in several ways and the ZX-calculus provides short proofs of their equivalence. For example, the original scheme describes a  $\wedge Z$  interaction between qubits initially prepared in the state  $|+\rangle$ ; in our notation this is  $Z_1^0$  or  $\bullet$ . Hence a one-dimensional cluster state can be presented diagrammatically as:



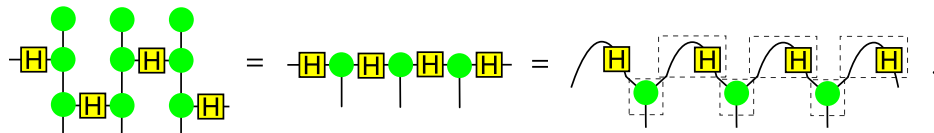
where the boxes delineate the individual  $|+\rangle$  preparations and  $\wedge Z$  operations. Alternatively, the cluster state can be prepared by applying a Hadamard gate to one part of a Bell pair to obtain states of the form  $|\Phi\rangle = |0+\rangle + |1-\rangle$ , and then ‘fusing’ these entangled pairs [76]. The required fusion operation is exactly

$$\bullet : \mathcal{Q} \otimes \mathcal{Q} \rightarrow \mathcal{Q} :: \begin{cases} |00\rangle & \mapsto |0\rangle \\ |11\rangle & \mapsto |1\rangle \\ |01\rangle, |10\rangle & \mapsto 0 \end{cases}, \tag{9}$$

and a 1D cluster prepared with this method looks like:



Again, dashed lines indicate the individual components. Whereas conventional methods require some calculation to show that these methods of preparation produce the same state, using the spider theorem, the two diagrammatic forms are immediately equivalent:



From the example of the 1D cluster, it is easy to see how to construct diagrams corresponding to arbitrary graph states. Indeed given a graph state  $|G\rangle$ , with the underlying graph  $G$ , we represent  $|G\rangle$  by the same graph  $G$ , with green dots at each vertex and  $H$  gates on each edge; to complete the construction we must add one output wire at each green vertex.

While graph states are important in measurement-based quantum computation, they are not the only kind of interesting entangled states. As an illustration of universality of the graphical language, we present graphical representatives of the two non-comparable classes of genuine

three-qubit entangled states<sup>5</sup>. As can be directly read from the interpretation given in section 2.3, the GHZ state is simply a three-legged spider:

$$|\text{GHZ}\rangle = |000\rangle + |111\rangle = \text{[Diagram: A green circle with three legs extending downwards, representing a spider.]}$$

The simple form of this state hints at its importance for the algebraic structures to be introduced later in this paper. This algebraic role, particularly in relation to the phase group, has been used to explain non-locality [20]. The W state, however, is less obvious:

$$|\text{W}\rangle = |001\rangle + |010\rangle + |100\rangle = \text{[Diagram: A green circle with three legs extending downwards. Each leg is connected to a red circle labeled \pi/3. The red circles are connected to each other in a triangle, representing pairwise entanglement.]}$$

This representation supports the intuition that while the GHZ state is globally entangled, the W is rather to be conceived as a pairwise entanglement between each pair of qubits that make up the three-partite system [38]. The algebraic properties of the W state have been studied elsewhere by Kissinger and one of the present authors [21].

**3.3.4. The one-way model.** The graphical language is ideal for studying different models of quantum computation in the same setting. In this section, we will present several computations using the one-way model [64], and translate them into equivalent quantum circuits using the rules of ZX-calculus. We use the *measurement calculus* notation introduced by Danos *et al* [30], and borrow their examples.

For our purposes, a measurement calculus program, called a *pattern*, consists of a sequence of commands of the following kinds:

- $N_i$ —initialize qubit  $i$  to the state  $|+\rangle$ ,
- $E_{ij}$ —apply a  $\wedge Z$  operation to qubits  $i$  and  $j$ ,
- $M_i^\alpha$ —measure the qubit  $i$  in the basis  $|0\rangle \pm e^{i\alpha}|1\rangle$ .

The commands occur in the order given: first initializations, then entanglement and then measurement. Any qubit that is not initialized is an input; any not measured is an output.

Since, in the ZX-calculus, measurements are replaced by projections, the conditional operations of the measurement calculus have been omitted; see section 12 and [37] for a more complete treatment. We make the convention that the observed outcome of each measurement will be the +1 outcome—that is, the projection onto  $|0\rangle + e^{i\alpha}|1\rangle$ . With this convention the elements of the measurement calculus can be translated by the following table:

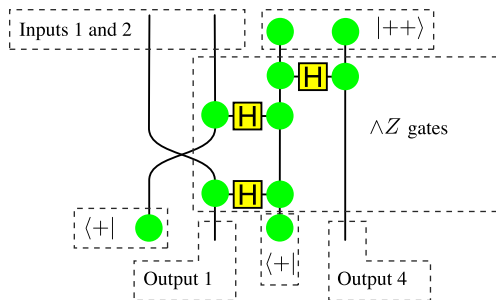
$N_i$	$E_{ij}$	$M_i^\alpha$

<sup>5</sup> The GHZ state cannot be converted to the W state by means of stochastic local operations and classical communication, nor vice versa. States that can be so interconverted are called *SLOCC-equivalent*: up to SLOCC-equivalence the GHZ and W are the *only* three-qubit states with three-party entanglement [38].

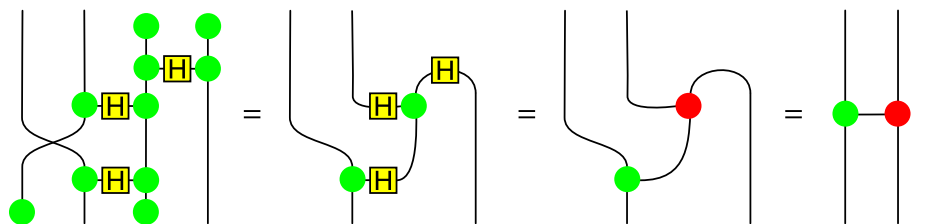
**Example 3.10.** Consider a measurement-based program involving four qubits, which computes a  $\wedge X$  gate upon its inputs. In the syntax of the measurement calculus, this pattern is written as

$$M_2^0 M_4^0 E_{13} E_{23} E_{34} N_3 N_4.$$

Reading from right to left, this specifies that qubits 3 and 4 should be prepared in a  $|+\rangle$  state, then  $\wedge Z$  operations should be applied pairwise between qubits 1 and 3, 2 and 3 and 3 and 4; finally  $X$  basis measurements should be performed upon qubits 2 and 4. Qubits 1 and 2 are the inputs and qubits 1 and 4 are the outputs. We represent this pattern diagrammatically as



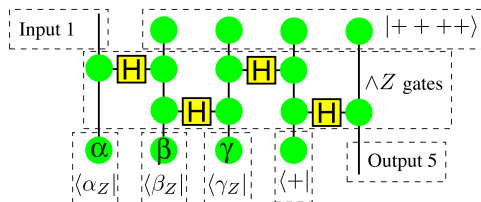
The spider theorem allows this one-way program to be rewritten to a  $\wedge X$  gate in three steps:



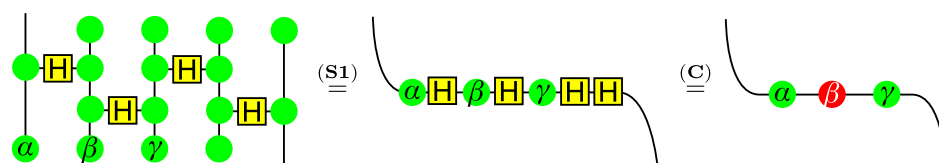
**Example 3.11.** Our next example is a one-way program implementing an arbitrary one-qubit unitary. Recall that any single-qubit unitary map  $U$  has a Euler decomposition such that  $U = Z_\gamma X_\beta Z_\alpha$ . Such a unitary can be implemented by the following five-qubit measurement pattern:

$$M_3^\gamma M_2^\beta M_1^\alpha E_{12} E_{23} E_{34} E_{45} N_2 N_3 N_4 N_5.$$

The graphical form of this pattern is shown below:



A sequence of simple rewrites shows that the one-way program intended to compute such a unitary does indeed produce the desired map.



**Remark 3.12.** *The reader may object that the ‘post-selection’ of one particular set of measurement outcomes reduces the number of diagrams significantly and thus gives a misleading air of feasibility to these techniques. In practice, the pure state version of the ZX-calculus needs only a minor extension to handle the full behaviour of the one-way model, without any combinatorial explosion. We sketch this extension in section 12; full details can be found in [37].*

#### 4. Symmetric monoidal categories and graphical reasoning

The preceding sections presented the ZX-calculus as a *fait accompli*, without any serious justification for its axioms other than its utility in certain calculations. This section, and those that follow, will present the firm mathematical foundation upon which the calculus is built. This section will outline the basic concepts of SMCs without going into too much technical detail; we aim to provide the reader with just enough background to follow the subsequent material, and provide many references where complete and detailed expositions can be found.

A *category* consists of *objects*  $A, B, C, \dots$  and, for each pair of objects  $A, B$ , a collection of *morphisms*  $f, g, h, \dots : A \rightarrow B$ . From a physical perspective, the objects can be thought of as *physical systems* and each morphism  $f : A \rightarrow B$  as a physical process that transforms a system of type  $A$  to a system of type  $B$ . Here, ‘type’ should not be confused with ‘state’. For example, ‘type’ could be a qubit or a field or a certain classical system, and each of these admits many states. For a computer scientist, the objects may be data types, and  $f : A \rightarrow B$  would be a program accepting input of type  $A$  and producing output of type  $B$ . In mathematics the objects are typically structures of a certain kind, e.g. sets or groups or vector spaces, and  $f : A \rightarrow B$  is a structure-preserving map, e.g. a function or a group homomorphism or a linear map.

Pairs of morphisms where the domain of one matches the codomain of the other may be *composed*: for each such pair,  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , we write the composite  $g \circ f : A \rightarrow C$ . In the case of physical processes  $g \circ f$  can be interpreted as ‘process *g* after process *f*’; in the case of structure-preserving maps the composition of morphisms is just ordinary function composition. Composition is assumed to be associative. One also assumes the existence of units for this composition; more precisely, for all  $A$  there exist identity morphisms  $1_A : A \rightarrow A$  such that for all  $f : A \rightarrow B$  and all  $g : B \rightarrow A$  we have  $f \circ 1_A = f$  and  $1_A \circ g = g$ . As a physical process this would stand for the *void* process, or in operational terms, ‘doing nothing’<sup>6</sup>.

In addition to the ‘sequential’ composition operation  $-\circ-$ , an SMC also comes with ‘parallel’ composition  $-\otimes-$ . For two physical systems  $A$  and  $B$  there is a *compound system*  $A \otimes B$  and for each pair of physical processes  $f : A \rightarrow C$  and  $g : B \rightarrow D$  there is a *compound process*  $f \otimes g : A \otimes B \rightarrow C \otimes D$ . For mathematical objects,  $\otimes$  then indicates a compound mathematical object of a certain kind, built from two ‘smaller’ ones, e.g. using the Cartesian product of sets or the direct product of groups or the tensor product of vector spaces. One also assumes a *unit object*  $I$ , which is such that composing  $A$  with  $I$ , one leaves  $A$  essentially unchanged. Finally, for each pair of objects  $A$  and  $B$ , one assumes

<sup>6</sup> Obviously, ‘doing nothing’ in the laboratory is a very difficult (if not impossible) task, e.g. preventing decoherence is the biggest stumbling block to building a quantum computer.

a *swap morphism*  $\sigma_{A,B}: A \otimes B \rightarrow B \otimes A$ . The remaining axioms of an SMC then play two roles:

- *bifunctionality* states how the two modes of composition interact;
- the existence of a number of *natural isomorphisms* and *coherence conditions* between these formalize the meaning of ‘essentially’ when saying that  $A \otimes I$  is ‘essentially’ the same as  $A$ .<sup>7</sup> The swap morphisms are also natural isomorphisms; these embody the canonical connection between  $A \otimes B$  and  $B \otimes A$ .<sup>8</sup>

All of these conditions have a straightforward physical interpretation and are satisfied for most standard mathematical constructions of compound objects.

Since there are two modes of composition, SMCs naturally lend themselves to a two-dimensional syntax we call the *graphical* (or *diagrammatic*) *calculus*, where the vertical axis corresponds to the sequential composition ‘ $\circ$ ’, and the horizontal axis to the tensor product ‘ $\otimes$ ’. Moreover, when expressed in the graphical language, the coherence conditions for SMCs become trivial as a consequence of some very powerful theorems, so they play no further role in this paper. Hence, while below we do state the symbolic definition of a symmetric monoidal category, it is not crucial for the remainder of this paper. The graphical language is both clearer and closer to the physical intuition; the reader who prefers the graphical language can skip ahead to section 4.3.

A more detailed account of the physical intuition behind SMCs can be found in [14, 17, 24]. The work [24] is an extensive tutorial specifically written to provide the appropriate background on the kind of category that is required for this paper. Other tutorials that may be of help are [3, 6]. Mac Lane’s standard textbook on category theory is of interest to a mathematical audience [57].

The graphical calculus for SMCs can be traced back to Penrose’s work in the early 1970s [61], but it was turned into a formal discipline only after the work of Freyd and Yetter, and Joyal and Street, was published around 1990 [42, 47]. A physicist-friendly presentation is again given in [14, 17, 24], and a specifically targeted tutorial is given in [24]. A recent comprehensive survey paper on graphical languages for more general monoidal categories, which settles a number of caveats of the earlier literature, is [69]. The reader interested in learning more may also find [6, 53, 73] helpful.

#### 4.1. Symmetric monoidal categories

**Definition 4.1.** A category  $\mathbf{C}$  consists of a class of objects denoted by  $|\mathbf{C}|$ , and for each pair of objects  $A, B \in |\mathbf{C}|$ , a set  $\mathbf{C}(A, B)$  of morphisms or arrows. For each triple  $A, B, C \in |\mathbf{C}|$  there is the composition

$$-\circ- : \mathbf{C}(A, B) \times \mathbf{C}(B, C) \rightarrow \mathbf{C}(A, C),$$

which is associative, i.e.  $(f \circ g) \circ h = f \circ (g \circ h)$ , and for each object  $A \in |\mathbf{C}|$  there is an identity morphism  $1_A : A \rightarrow A$ ; that is, for all  $f \in \mathbf{C}(A, B)$  we have  $f \circ 1_A = f = 1_B \circ f$ .

<sup>7</sup> For example, although for all practical purposes the sets  $X \times (Y \times Z)$  and  $(X \times Y) \times Z$  are equivalent, they are strictly speaking not the same: the first one contains elements of the form  $(x, (y, z))$  while the second one contains elements of the form  $((x, y), z)$ . Making this notion of equivalence mathematically precise is what makes the explicit definition of an SMC somewhat heavy-handed.

<sup>8</sup> Now,  $(x, y)$  and  $(y, x)$  are no longer ‘essentially the same’, but they still are canonically connected via the operation ‘swapping elements’.

A morphism  $f : A \rightarrow B$  has *domain*  $A$  and *codomain*  $B$ . We will sometimes refer to objects as *types*, to  $A$  as the *input type* and to  $B$  as the *output type*.

In order to precisely state the definition of an SMC we need to introduce two auxiliary concepts: functors and natural transformations. While these definitions may seem rather abstract, the only examples of them that will be needed are familiar ones: the tensor product, and isomorphisms between tensor products of objects.

By explicitly stating some basic category-theoretic notions the reader may get a sense of why even many mathematicians consider category theory as ‘very abstract’; in contrast, the diagrammatic calculus shows that specific parts of category theory, namely SMCs and in particular their graphical calculus, can make certain mathematical structures much more intuitive and easier to manipulate.

**Definition 4.2.** Let  $\mathbf{C}$  and  $\mathbf{D}$  be categories. A functor  $F : \mathbf{C} \rightarrow \mathbf{D}$  is defined by (i) for each object  $A$  in  $|\mathbf{C}|$  an object  $F(A)$  in  $|\mathbf{D}|$ , and (ii) for every arrow  $f : A \rightarrow B$  in  $\mathbf{C}$  an arrow  $F(f) : F(A) \rightarrow F(B)$  in  $\mathbf{D}$  such that:

$$F(f \circ g) = F(f) \circ F(g) \quad \text{and} \quad F(1_A) = 1_{F(A)}.$$

**Remark 4.3.** A variation on the idea of functor is a *contravariant functor*, which reverses the direction of arrows; that is,  $F$  assigns to every arrow  $f : A \rightarrow B$  in  $\mathbf{C}$  an arrow  $F(f) : F(B) \rightarrow F(A)$  in  $\mathbf{D}$ .

**Definition 4.4.** A *bifunctor* is a functor of two arguments  $F : \mathbf{C} \times \mathbf{C}' \rightarrow \mathbf{D}$ , that is a functor in each argument separately, i.e., for all objects  $X$  and arrows  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  in  $\mathbf{C}$ , and all objects  $X'$  and arrows  $f' : A' \rightarrow B'$ ,  $g' : B' \rightarrow C'$  in  $\mathbf{C}'$ , we have:

$$\begin{aligned} F(g, 1_{X'}) \circ F(f, 1_{X'}) &= F(g \circ f, 1_{X'}), \\ F(1_X, g') \circ F(1_X, f') &= F(1_X, g' \circ f'), \end{aligned}$$

which additionally satisfies

$$\begin{aligned} F(g, 1_{B'}) \circ F(1_B, f') &= F(1_C, f') \circ F(g, 1_{A'}), \\ F(1_A, 1_{B'}) &= 1_{F(A, B')}. \end{aligned}$$

In essence, a functor is a map between categories that preserves the structure of the category, i.e. composition and identities. We will also need maps between functors.

**Definition 4.5.** Let  $F, G : \mathbf{C} \rightarrow \mathbf{D}$  be functors; a *natural transformation*  $\tau : F \rightarrow G$  is a family of arrows in  $\mathbf{D}$ ,  $\tau_A : F(A) \rightarrow G(A)$ , indexed by the objects of  $\mathbf{C}$ , such that the following square commutes:

$$\begin{array}{ccc} F(A) & \xrightarrow{\tau_A} & G(A) \\ F(f) \downarrow & & \downarrow G(f) \\ G(A) & \xrightarrow{\tau_B} & G(B), \end{array}$$

for all arrows  $f : A \rightarrow B$  in  $\mathbf{C}$ . A *natural isomorphism* is a natural transformation where each of the  $\tau_A$  is an isomorphism; that is, there exists a morphism  $\tau_A^{-1}$  such that  $\tau_A \circ \tau_A^{-1}$  and  $\tau_A^{-1} \circ \tau_A$  are both identities.



*Notation and terminology:* Each directed path in the diagram above determines a composition of two maps:  $G(f) \circ \tau_A$  on the upper path and  $\tau_B \circ F(f)$  on the lower. The phrase ‘the square commutes’ means that both paths in this directed graph are equal, i.e.  $G(f) \circ \tau_A = \tau_B \circ F(f)$ .

If two objects in category are naturally isomorphic then they are isomorphic, ‘for structural reasons’ and not because of any particular details of the objects themselves. The following definition provides a key example.

**Definition 4.6.** A monoidal category  $(\mathbf{C}, \otimes, \mathbf{I})$  is a category  $\mathbf{C}$  equipped with a bifunctor  $-\otimes- : \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ , a distinguished unit object  $\mathbf{I}$ , natural unit isomorphisms

$$\lambda_A: A \simeq \mathbf{I} \otimes A \quad \text{and} \quad \rho_A: A \simeq A \otimes \mathbf{I},$$

and a natural associativity isomorphism

$$\alpha_{A,B,C}: A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C,$$

which are subject to certain coherence equations, which we omit.

The bifunctor  $-\otimes-$  is called the *tensor product* or *monoidal tensor*. The maps  $\lambda$ ,  $\rho$  and  $\alpha$  are called the monoidal *structure maps*. A monoidal category is called *strict* when the structure maps are all identities; that is, when the objects made isomorphic by  $\lambda$ ,  $\rho$  and  $\alpha$  are in fact equal. The following theorem by Mac Lane justifies our omission of the coherence equations for the structure maps.

**Theorem 4.7.** Every monoidal category is equivalent to a strict monoidal category.

For details we refer the reader to [57]. Henceforward all the monoidal categories we consider will be strict, although we will frequently use the symbols  $\lambda_A$  and  $\rho_A$  for clarity, for example, when composing an arrow of type  $B \rightarrow A$  with one of type  $A \otimes I \rightarrow C$ .

**Definition 4.8.** A symmetric monoidal category is a monoidal category equipped with a natural symmetry isomorphism

$$\sigma_{A,B}: A \otimes B \simeq B \otimes A$$

such that  $\sigma_{A,B}^{-1} = \sigma_{B,A}$  and again subject to some coherence conditions which we omit.

If  $\mathbf{C}$  is an SMC, then  $\sigma$  is counted among its structure maps. Unlike the other structure maps,  $\sigma$  cannot be replaced by the identity without losing essential structure. Again see [57] for details of the coherence conditions, which are summarized in the following theorem [52]:

**Theorem 4.9** (Kelly–Mac Lane). Let  $f$  and  $g$  be parallel natural isomorphisms in a symmetric monoidal category, both constructed from identities and the structure maps by tensoring and composition; then  $f = g$ .

Essentially, this result says that when one uses the structure maps to permute the factors of a tensor product, only the permutation matters, not how it was constructed.<sup>9</sup>

The preceding definitions may seem rather intimidating to those unfamiliar with category theory, but there is no need to be alarmed: SMCs are among the most ubiquitous of mathematical structures!

<sup>9</sup> The restriction to *natural* isomorphisms prevents different permutations from being identified. For example,  $1_{A \otimes A}$  and  $\sigma_{A,A}$  cannot be identified, despite being parallel arrows, since they are components of *different* natural transformations, namely  $1 \otimes 1: A \otimes B \Rightarrow A \otimes B$  and  $\sigma: A \otimes B \Rightarrow B \otimes A$ ; again see [57] for details.

**Example 4.10.** The SMC  $(\mathbf{FdHilb}, \otimes, \mathbb{C})$ , often written simply as  $\mathbf{FdHilb}$ , has finite dimensional Hilbert spaces as objects and linear maps as its morphisms, which compose by ordinary composition of linear maps. The familiar Kronecker tensor product is the monoidal tensor, and the field of complex numbers  $\mathbb{C}$ —which is a 1D Hilbert space over itself—is the tensor unit.

The requirement that the monoidal tensor be a bifunctor reduces to the following well-known property of linear maps:

$$(f \otimes g) \circ (h \otimes k) = (f \circ h) \otimes (g \circ k).$$

We indeed also have  $\mathcal{H} \simeq \mathbb{C} \otimes \mathcal{H}$  via the natural isomorphism:

$$\begin{aligned} \lambda_{\mathcal{H}} : \mathcal{H} &\rightarrow \mathbb{C} \otimes \mathcal{H} :: |\psi\rangle \mapsto 1 \otimes |\psi\rangle, \\ \lambda_{\mathcal{H}}^{-1} : \mathbb{C} \otimes \mathcal{H} &\rightarrow \mathcal{H} :: c \otimes |\psi\rangle \mapsto c|\psi\rangle, \end{aligned}$$

where naturality means that for all  $f : \mathcal{H} \rightarrow \mathcal{H}'$  the following diagram commutes:

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{\lambda_{\mathcal{H}}} & \mathbb{C} \otimes \mathcal{H} \\ f \downarrow & & \downarrow 1_{\mathbb{C}} \otimes f \\ \mathcal{H}' & \xrightarrow{\lambda_{\mathcal{H}'}} & \mathbb{C} \otimes \mathcal{H}' \end{array}$$

i.e.  $(1_{\mathbb{C}} \otimes f) \circ \lambda_{\mathcal{H}} = \lambda_{\mathcal{H}'} \circ f$ . In  $\mathbf{FdHilb}$ , it is easily checked that natural transformations are always basis independent. See [24] for a detailed description of  $(\mathbf{FdHilb}, \otimes, \mathbb{C})$ .

**Example 4.11.** Let  $(\mathbf{ZX}, \otimes, 0)$  denote the SMC whose objects are natural numbers, and whose arrows  $f : n \rightarrow m$  are diagrams of the ZX-calculus, as described in section 2, with  $n$  inputs and  $m$  outputs. The identity arrows are diagrams consisting of straight wires from inputs to outputs, and composition is achieved by plugging inputs to outputs.

The tensor product on objects is addition  $n \otimes m := n + m$ , and the unit object is zero:  $n \otimes 0 = n + 0 = n$ . Tensor product of two diagrams is juxtaposition, and the identity map  $1_0$  is just the empty diagram. By its construction,  $\mathbf{ZX}$  is evidently a strict monoidal category. We leave to the reader the task of constructing the symmetry maps  $\sigma_{n,m}$  from crossings of wires.

We remark in passing that the assignment from a diagram  $\mathcal{D}$  to its corresponding linear map  $D$ , described in section 2.3, defines a functor from  $\mathbf{ZX}$  to  $\mathbf{FdHilb}$ .

In the categorical setting, the internal structure of the objects is hidden—abstracted away; the state spaces are effectively reduced to labels which determine when morphisms may be composed. However, in  $\mathbf{FdHilb}$  and many other important examples, the internal structure of the spaces may be reconstructed via the structure of the morphisms into that space.

**Definition 4.12.** Morphisms of type  $I \rightarrow A$  in a monoidal category  $\mathcal{C}$  are called points of  $A$ .

**Example 4.13.** Any linear map  $\psi : \mathbb{C} \rightarrow \mathcal{H}$  is completely determined by  $\psi(1)$ , due to linearity; hence there is a bijection,

$$\mathbf{FdHilb}(\mathbb{C}, \mathcal{H}) \rightarrow \mathcal{H} :: \psi \mapsto \psi(1).$$

So the elements of  $\mathbf{FdHilb}(\mathbb{C}, \mathcal{H})$  are the points of the object  $\mathcal{H}$ . To distinguish between the linear map  $\psi$  and the vector  $\psi(1)$  we will denote the latter by  $|\psi\rangle$ . As processes, we can think of these points  $\psi : \mathbb{C} \rightarrow \mathcal{H}$  also as preparation procedures.

A point  $\Psi: I \rightarrow A \otimes B$  is a state of the compound system  $A \otimes B$ , and this state may or may not be entangled. If it is not entangled, then we have

$$\Psi = (\psi_A \otimes \psi_B) \circ \lambda_I,$$

that is, the state  $\Psi$  factors in state  $\psi_A$  of system  $A$  and state  $\psi_B$  of system  $B$ . It is entangled if such a factorization does not exist. If the category bears a certain additional structure, e.g. compactness as described in section 4.4, then the existence of entangled states can be guaranteed, which in turn enables the derivation of teleportation-like protocols [1].

In many categories, the points can reveal a great deal about the arrows. For example, in a vector space, two linear maps are equal if they agree on a small number of points, namely a basis. To tell if two functions are equal, it suffices to evaluate them on every element of their domain. The analogous procedure is not possible in every category. More precisely, a set of points  $\mathcal{K} \subseteq \mathbf{C}(I, A)$  is called a *basis* for  $A$  if for all objects  $B$ , and all arrows  $f, g: A \rightarrow B$ , we have

$$[\forall k \in \mathcal{K}: f \circ k = g \circ k] \text{ implies } f = g.$$

If every object of  $\mathbf{C}$  has a basis, then we say that  $\mathbf{C}$  has *enough points*. Fortunately, the examples of interest here *do* have enough points, and section 5 describes the particular forms of bases that will be of interest in later sections.

**Definition 4.14.** *Let  $\mathbf{C}$  be a monoidal category; the arrows of type  $I \rightarrow I$  are called the scalars of  $\mathbf{C}$ . Given a scalar,  $c: I \rightarrow I$ , we call the natural transformation with components*

$$c \cdot 1_A := \lambda_A^{-1} \circ (c \otimes 1_A) \circ \lambda_A: A \rightarrow A$$

*the scalar multiplication by  $c$ .*

More explicitly, we can define

$$c \cdot f := f \circ (c \cdot 1_A) = (c \cdot 1_B) \circ f = \lambda_B^{-1} \circ (c \otimes f) \circ \lambda_A \quad (10)$$

to be the scalar multiplication of morphism  $f: A \rightarrow B$  by the scalar  $c$ .

The scalars, in any monoidal category, form a commutative monoid with respect to composition [51]. From the definition of scalar multiplication it follows that

$$(c \cdot f) \circ (c' \cdot g) = (c \circ c') \cdot (f \circ g), \quad (11)$$

$$(c \cdot f) \otimes (c' \cdot g) = (c \circ c') \cdot (f \otimes g). \quad (12)$$

Intuitively, in the language of SMCs, if a scalar appears in the description of a morphism, it does not matter where it appears: its effect is that of a global multiplier for the entire morphism.

**Example 4.15.** *In  $\mathbf{FdHilb}$  the scalars are the complex numbers. Indeed, a linear map  $c: \mathbb{C} \rightarrow \mathbb{C}$  is completely determined by  $c(1)$ , due to linearity, so there is a bijection*

$$\mathbf{FdHilb}(\mathbb{C}, \mathbb{C}) \rightarrow \mathbb{C} :: c \mapsto c(1).$$

*Scalar multiplication as in (10) coincides with the usual linear algebraic notion, for which (11) and (12) indeed hold. The commutative monoid of scalars is isomorphic to the monoid of the complex numbers  $(\mathbb{C}, \cdot, 1)$ . For more details, again see [24].*

## 4.2. The $\dagger$ functor

Following [1, 2, 68], we augment SMCs with additional structure that plays an essential role in the quantum mechanical formalism.

**Definition 4.16.** A  $\dagger$ -symmetric monoidal category ( $\dagger$ -SMC) is a symmetric monoidal category equipped with an identity-on-objects contravariant endofunctor

$$(-)^\dagger : \mathbf{C}^{op} \rightarrow \mathbf{C},$$

which assigns to each morphism  $f: A \rightarrow B$  an adjoint morphism  $f^\dagger: B \rightarrow A$ , which coherently preserves the monoidal structure, that is,

$$(f \circ g)^\dagger = g^\dagger \circ f^\dagger, \quad (f \otimes g)^\dagger = f^\dagger \otimes g^\dagger, \quad 1_A^\dagger = 1_A, \quad f^{\dagger\dagger} = f.$$

Further, for the natural isomorphisms  $\lambda$ ,  $\rho$ ,  $\alpha$  and  $\sigma$  of the symmetric monoidal structure, the adjoint and the inverse coincide.

**Definition 4.17.** If for an isomorphism  $f: A \rightarrow B$  in a  $\dagger$ -SMC the adjoint and the inverse coincide, that is,  $f^\dagger = f^{-1}$ , then we call it unitary.

**Remark 4.18.** In a  $\dagger$ -SMC, the monoid of scalars is involutive; that is, there is an operation  $\dagger : \mathbf{C}(\mathbf{I}, \mathbf{I}) \rightarrow \mathbf{C}(\mathbf{I}, \mathbf{I})$  that satisfies

$$(c \circ d)^\dagger = d^\dagger \circ c^\dagger, \quad 1_{\mathbf{I}}^\dagger = 1_{\mathbf{I}}, \quad c^{\dagger\dagger} = c.$$

**Example 4.19.** In  $\mathbf{FdHilb}$ , the  $\dagger$  functor is given by the adjoints of linear algebra. The involution for the monoid of scalars is complex conjugation.

The category  $\mathbf{FdHilb}$  is obviously not the only example of a  $\dagger$ -SMC; by its construction,  $\mathbf{ZX}$  is a  $\dagger$ -SMC. We offer some further examples.

**Example 4.20** (relations). Recall that for two relations  $r \subseteq X \times Y$  and  $s \subseteq Y \times Z$  the relational composite is again a relation:

$$s \circ r := \{(x, z) \mid \exists y: (x, y) \in r, (y, z) \in s\} \subseteq X \times Z.$$

The category  $\mathbf{Rel}$  that has sets as objects, relations as morphisms and relational composition is a  $\dagger$ -SMC with the Cartesian product of sets as the monoidal structure, and the relational converse as the  $\dagger$  functor. The unit object for the monoidal structure is the singleton set  $\{*\}$ , since  $X \times \{*\} \simeq X$  for any set  $X$ , and the monoid of scalars is now isomorphic to the Boolean monoid  $(\mathbb{B}, \wedge, 1)$ , since there are only two relations  $r: \{*\} \rightarrow \{*\}$ , namely the empty relation and the identity relation. The involution for the monoid of scalars is now trivial. We write  $\mathbf{FRel}$  when restricting to finite sets. In  $\mathbf{Rel}$  the points of an object  $X$  are not its elements but its subsets—a detailed discussion is given in [14, 24]. While at first sight  $(\mathbf{F})\mathbf{Rel}$  seems to have little to do with physics, it enables one to encode a surprising number of quantum phenomena. For example, Spekkens' toy quantum theory [72] can be embedded within it as a sub- $\dagger$ -SMC  $\mathbf{Spek}$  [19, 20]. This succinct categorical presentation of this toy theory is moreover the only currently available rigorous mathematical presentation of it.

**Example 4.21** (projective spaces). *The passage from vectors to states comes with a radical change of the mathematical description of the spaces: from vector spaces to projective spaces, which drove von Neumann into the advent of lattice theory and quantum logic [9, 66]. Meanwhile, 75 years later, it is fair to say that the quantum logic research programme failed in reaching its ambitious goals, the main problem being the failure to account for the tensor product description of compound quantum systems. However, at the level of monoidal categories, which has the tensor built in as a primitive concept, the passage from vector spaces to projective spaces proceeds without any loss of the structures that play a role in this paper [15]. Let  $\mathbf{FdHilb}_p$  be the category that has the same objects as  $\mathbf{FdHilb}$  but whose morphisms are equivalence classes of  $\mathbf{FdHilb}$ -morphisms, given by the equivalence relation*

$$f \sim g \Leftrightarrow \exists c \in \mathbb{C} \setminus \{0\} \text{ s.t. } f = c \cdot g.$$

*In  $\mathbf{FdHilb}_p$  the states are now indeed the rays of the Hilbert space, together with one point representing the zero vector. The points for the two-dimensional Hilbert space in  $\mathbf{FdHilb}_p$ , the set  $\mathbf{FdHilb}_p(\mathbb{C}, \mathbb{C}^2)$ , correspond to the points of the Bloch sphere.*

*Operationally, the meaningful scalars are the probability amplitudes. In  $\mathbf{FdHilb}$ , the scalars are the complex numbers, hence too many, and in  $\mathbf{FdHilb}_p$  there are only two, hence too few. The solution consists of enriching  $\mathbf{FdHilb}_p$  with probabilistic weights, i.e. to consider morphisms of the form  $r \cdot f$ , where  $r \in \mathbb{R}^+$  and  $f$  a morphism in  $\mathbf{FdHilb}_p$ . Therefore, let  $\mathbf{FdHilb}_{wp}$  be the category whose objects are those of  $\mathbf{FdHilb}$  and whose morphisms are equivalence classes of  $\mathbf{FdHilb}$ -morphisms for*

$$f \sim g \Leftrightarrow \exists \alpha \in [0, 2\pi) \text{ s.t. } f = e^{i\alpha} \cdot g.$$

*A detailed categorical account of  $\mathbf{FdHilb}_{wp}$  is given in [15].*

*The three categories considered above are related via inclusions:*

$$\mathbf{FdHilb}_p \begin{array}{c} \xleftarrow{\quad} \\ \hookrightarrow \end{array} \mathbf{FdHilb}_{wp} \begin{array}{c} \xleftarrow{\quad} \\ \hookrightarrow \end{array} \mathbf{FdHilb}.$$

*The theorems proven in this paper apply to all of these.*

**Example 4.22** (mixed states and completely positive maps). *In this paper, all processes are pure (or closed). However, given any  $\dagger$ -SMC  $\mathbf{C}$  of ‘pure states’ it is possible to construct a new category  $\mathbf{CPM}(\mathbf{C})$  of mixed states and completely positive maps which is again a  $\dagger$ -SMC. This method, Selinger’s CPM-construction [68], will be sketched in section 12.1.*

### 4.3. Diagrammatic calculus

In diagrammatic calculus, morphisms in SMCs are represented by *boxes*, input types by *input wires* and output types by *output wires*. Identities can be represented by wires only. Hence,  $1_A: A \rightarrow A$  and  $f: A \rightarrow B$  are, respectively, depicted as

$$\begin{array}{c} A \\ | \\ A \end{array} \quad \begin{array}{c} A \\ \boxed{f} \\ B \end{array} . \tag{13}$$



This correspondence instantiates a perfect correspondence between the symbolic representation and the graphical presentation of SMCs:

**Theorem 4.24** (Joyal–Street [47]). *An equation expressed in the symbolic language of SMCs follows from the axioms of SMCs if and only if it holds up to isomorphism of diagrams in the graphical language.*

As Selinger pointed out in [68], this result straightforwardly extends to  $\dagger$ -SMCs, when representing the adjoint by vertical reflection. This requires breaking the symmetry of the boxes used above, and  $f: A \rightarrow B$  and  $f^\dagger: B \rightarrow A$  will now be, respectively, depicted as

$$\begin{array}{c} A \\ | \\ \boxed{f} \\ | \\ B \end{array} \quad \begin{array}{c} B \\ | \\ \boxed{f} \\ | \\ A \end{array} . \quad (19)$$

Note that reflecting twice leaves the box invariant, exposing the involutive nature of the adjoint.

#### 4.4. Graphical reasoning

In the following sections, the graphical language will be preferred to conventional linear syntax. Before proceeding, we briefly discuss the question of equational reasoning in the graphical language: when do two diagrams denote the same mathematical object? When are two diagrams equal? There are two basic elements: *isomorphism of diagrams*, as discussed above; and *substitution*. Together these principles allow us to reason by *rewriting*.

The first principle, isomorphism, requires little elaboration beyond the discussion of section 4.3. The graphical language is a syntax for describing certain mathematical objects, namely the arrows of symmetric monoidal categories; theorem 4.24 states that two diagrams denote equal arrows when they are isomorphic (in the sense of definition 4.23).

However, the axioms of SMCs are rather weak, so the isomorphism principle will not suffice. We must impose other equations on our diagrams to obtain our results. For example, consider an arrow  $f: A \rightarrow A$ . The statement that  $f$  is unitary is expressed by the equations

$$f \circ f^\dagger = 1_A = f^\dagger \circ f. \quad (20)$$

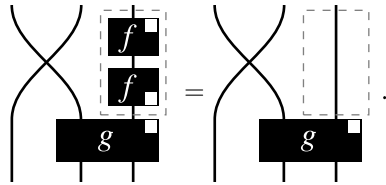
Since this equation is a property of the particular morphism  $f$ , there is no hope to absorb it into some overarching global principle, in the way that theorem 4.24 absorbs the axioms of SMCs. Indeed, most of the equations in this paper are of this sort, naked identifications that must be imposed on the language. We deal with these via substitution.

From a syntactic point of view, the meaning of an equation such as (20) is that whenever  $f^\dagger \circ f$  is found lurking inside some larger expression, it can be replaced by  $1_A$  without changing the meaning of the containing expression. The same method of substitution applies in the graphical language.

The equations above can be easily translated into diagrams:

$$\begin{array}{c} \boxed{f} \\ | \\ \boxed{f} \end{array} = | = \begin{array}{c} \boxed{f} \\ | \\ \boxed{f} \end{array} .$$

To perform the substitution, we isolate the part of the diagram corresponding to one side of the equation, and form a new diagram by replacing that part with the other side of the equation.



Since two equal diagrams must have the same type, such a replacement is always possible.

In general, when presented with a diagram  $d$ , any vertical line (which does not intersect any box or wire) divides the diagram into two parts,  $f$  and  $g$ , each of which is a valid diagram, and which are related by the equation  $d = f \otimes g$ . Similarly, any horizontal line (which may cut wires, but avoids boxes and points where wires cross) will divide  $d$  into two sub-diagrams,  $f'$  and  $g'$ , which satisfy  $d = f' \circ g'$ . By a sequence of such horizontal and vertical divisions, the diagram can be cut into squares each of which contains an atomic element of the graphical language: a single box, a single crossing of wires or a single straight wire. Each atomic square corresponds to a single symbol in standard notation, and hence the factorization yields a symbolic expression equivalent to the diagram. The desired substitution can be performed on the symbolic expression, and a new diagram constructed. We can pass freely from the symbolic representation to the graphical representation and back.

$$(1_A \otimes g) \circ (\sigma \otimes (f^\dagger \circ f)) = (1_A \otimes g) \circ (\sigma \otimes 1_A).$$

The above justification for substitution is admittedly rather sketchy. Joyal and Street [47] provide a rigorous presentation with all the details. In practice, there is no need to divide a diagram into atomic pieces: it suffices to isolate the part to be substituted. We will apply this technique throughout this paper.

#### 4.5. Correctness of graphical reasoning in ZX-calculus

The cautious reader will be aware that the **T**-rule of the ZX-calculus in section 2—‘only the topology of the diagram matters’—stretches well beyond the graphical reasoning techniques outlined above. As well as being a  $\dagger$ -SMC, **ZX** has a richer structure, and enjoys a correspondingly stronger analogue to theorem 4.24.

**Definition 4.25.** A dagger compact (closed) category is a  $\dagger$ -SMC in which for each object  $A$  there exists dual object  $A^*$  and a morphism  $\eta_A: I \rightarrow A^* \otimes A$  subject to certain coherence equations (for which see [1, 68]).

Throughout this paper, we will take  $A^* = A$ ; this self-duality requires some additional coherence axioms, for which see [70].



For the present purposes the required equations reduce to a very simple form. Denoting  $\eta_A$  graphically by  $\frown$ , the equations that need to be satisfied are

$$\lambda_A^\dagger \circ (\eta^\dagger \otimes 1_A) \circ (1_A \otimes \eta) \circ \rho_A = 1_A, \quad \text{i.e.} \quad \text{U} = | \quad (21)$$

$$\sigma_{A,A} \circ \eta = \eta, \quad \text{i.e.} \quad \text{O} = \frown. \quad (22)$$

**Theorem 4.26** (Kelly–Laplaza [51]; Selinger [68, 70]). *An equation expressed in the symbolic language of the dagger compact category follows from the axioms of dagger compact categories if and only if it holds up to isotopy in the graphical language.*

This result may be used in the ZX-calculus due the last two equations of the **S2**-rule, which allows us to consider the caps and cups as part of the overall categorical structure. In what follows, these equations will typically not hold. A collection of many other theorems on diagrammatic languages can be found in [69].

## 5. Vector bases and state bases of observables

Before delving into the categorical treatment of observables, we briefly recall the relevant notions in the concrete setting of Hilbert space quantum mechanics. All Hilbert spaces involved will be finite dimensional. We will denote the set of rays in a Hilbert space  $\mathcal{H}$ , which we refer to as the *state space*, by  $\mathcal{H}$  itself. To distinguish between states and vectors, we write  $\llbracket \psi \rrbracket$  to denote the unique state containing the (non-zero) vector  $|\psi\rangle$ . Similarly,  $\llbracket \sum_i c_i |v_i\rangle \rrbracket$  is the state spanned by vector  $\sum_i c_i |v_i\rangle$ .

All observables considered will be non-degenerate:  $\hat{O} = \sum_i \lambda_i |v_i\rangle \langle v_i|$ . For the current purposes, the importance of the observable is the state change  $\llbracket \psi \rrbracket \mapsto \llbracket v_i \rrbracket$  induced by measuring it. Since the actual values  $\lambda_i$  are of no concern here, we identify an observable with its set of eigenstates,  $\{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\}$ . We refer to the orthonormal basis  $\{|v_1\rangle, \dots, |v_n\rangle\}$  as a *vector basis*, cf definition 5.3 below. To summarize:

vector	state	vector basis	observable
$ \psi\rangle$	$\llbracket \psi \rrbracket$	$\{ v_1\rangle, \dots,  v_n\rangle\}$	$\{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\}$

**Definition 5.1.** *A vector  $|\psi\rangle$  (or state  $\llbracket \psi \rrbracket$ ) is unbiased relative to a vector basis  $\{|v_1\rangle, \dots, |v_n\rangle\}$  (or observable  $\{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\}$ ) if for all  $i, j$  we have*

$$|\langle v_i | \psi \rangle| = |\langle v_j | \psi \rangle|.$$

*In particular, if  $\mathcal{H} = \mathbb{C}^D$ , then  $|\langle v_i | \psi \rangle| = 1/\sqrt{D}$  for all  $i$ . Two vector bases (or two observables) are complementary (or mutually unbiased) if each vector (or state) in one of these vector bases (or observables) is unbiased relative to the other vector basis (or observable).*

The key physical fact here is that when a state is unbiased to some observable, all the outcomes of that observable are equally likely. If classical data are encoded in the eigenbasis of some observable, for example a classical bit encoded as a qubit in the basis  $\{|0\rangle, |1\rangle\}$ , then

measuring an unbiased observable will effectively *erase* that data, regardless of which outcome is observed.

A vector basis of a Hilbert space is characterized by the following property:

**Proposition 5.2.** *Let  $\{|v_1\rangle, \dots, |v_n\rangle\}$  be any vector basis of a Hilbert space  $\mathcal{H}$ . Then, any linear map  $f: \mathcal{H} \rightarrow \mathcal{H}'$  is completely determined by the values  $f$  takes on  $|v_1\rangle, \dots, |v_n\rangle$ . Further, no proper subset  $\{|v_1\rangle, \dots, |v_n\rangle\}$  suffices to determine  $f$ .*

Any regular linear map induces a map from states to states, namely

$$\hat{f} :: \llbracket \psi \rrbracket \mapsto \llbracket f(|\psi\rangle) \rrbracket.$$

However, the values that  $\hat{f}$  takes on an observable  $\{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\}$  do not suffice to fix  $\hat{f}$  itself. For example, let  $\theta, \theta' \in [0, 2\pi)$ , and define a family of linear maps, relative to basis  $\{|0\rangle, |1\rangle\}$ , by the matrix:

$$f_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Every  $\hat{f}_\theta$  leaves both  $|0\rangle$  and  $|1\rangle$  invariant, while

$$\hat{f}_\theta(\llbracket + \rrbracket) = \llbracket |0\rangle + e^{i\theta}|1\rangle \rrbracket \neq \llbracket |0\rangle + e^{i\theta'}|1\rangle \rrbracket = \hat{f}_{\theta'}(\llbracket + \rrbracket)$$

whenever  $\theta \neq \theta'$ . Is there an analogue to proposition 5.2? Can  $\hat{f}$  be characterized by its image on some minimal set of states? The answer is yes:

**Definition 5.3.** *A set of states of the form*

$$\text{observable} \cup \{\text{unbiased state for that observable}\}$$

*is called a state basis. The unbiased state is called the erasing point.*

**Proposition 5.4.** *Any map on states  $\hat{f}$  induced by a regular linear map  $f: \mathcal{H} \rightarrow \mathcal{H}'$  is completely determined by the values it takes on a state basis for some arbitrary observable. Moreover, no proper subset of such a set of states suffices to determine  $\hat{f}$ .*

**Proof.** Let  $f$  be a regular linear map, and let  $\hat{f}$  be the corresponding map of states. Let  $\{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\} \cup \{\llbracket s \rrbracket\}$  form a state basis, and suppose that  $\hat{f}$  takes known values upon these states. We will show that this determines  $f$  on a vector basis  $\{|\eta_1\rangle, \dots, |\eta_n\rangle\}$  of  $\mathcal{H}$ , up to a common, overall phase.

Set  $|\eta_i\rangle = \langle v_i | s \rangle |v_i\rangle$  and let  $\mathcal{H}''$  be the subspace spanned by  $f(|\eta_1\rangle), \dots, f(|\eta_n\rangle)$ . Since  $f$  is regular  $\{f(|\eta_1\rangle), \dots, f(|\eta_n\rangle)\}$  is a basis for  $\mathcal{H}''$ , and let  $\langle - | - \rangle_\diamond$  denote the inner product on  $\mathcal{H}''$  for which  $\{f(|\eta_1\rangle), \dots, f(|\eta_n\rangle)\}$  is orthonormal. Then the codomain restriction of  $f$  to  $(\mathcal{H}'', \langle - | - \rangle_\diamond)$  is unitary. Relying on this we have  $f(|\eta_i\rangle) = f(\langle v_i | s \rangle |v_i\rangle) = \langle v_i | s \rangle f(|v_i\rangle) = \langle f(|v_i\rangle) | f(|s\rangle) \rangle_\diamond f(|v_i\rangle)$ . This expression is completely determined by  $\hat{f}(\llbracket v_i \rrbracket)$  and  $\hat{f}(\llbracket s \rrbracket)$  up to a phase factor contributed by  $f(|s\rangle)$ , but this phase factor is the same for all  $f(|\eta_i\rangle)$ .

It now follows that, given an arbitrary state  $\llbracket \psi \rrbracket = \llbracket \sum_i c_i |\eta_i\rangle \rrbracket$ , we have  $\hat{f}(\llbracket \psi \rrbracket) = \llbracket f(|\psi\rangle) \rrbracket = \llbracket f(\sum_i c_i |\eta_i\rangle) \rrbracket = \llbracket \sum_i c_i f(|\eta_i\rangle) \rrbracket$ , where each  $f(|\eta_i\rangle)$  is determined up to the common phase. This phase is therefore a global phase for the vector  $\sum_i c_i f(|\eta_i\rangle)$ ; hence  $\hat{f}(\llbracket \psi \rrbracket)$  yields a unique state, and so  $\hat{f}$  is well defined on all states.

It is easily seen that no proper subset of  $\{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket, \llbracket s \rrbracket\}$  is sufficient for completely determining  $\hat{f}$ .  $\square$

State bases and vector bases are related by the following proposition:

**Proposition 5.5.** *Let  $\mathcal{S}$  be the set of all state bases for  $\mathcal{H}$ , let  $\mathcal{V}$  be the set of all vector bases for  $\mathcal{H}$  and let  $\mathcal{V}/\sim$  be the set of equivalence classes  $[-]_{\sim}$  in  $\mathcal{V}$  for the equivalence relation ‘equal up to an overall phase’, i.e.*

$$\{|v_1\rangle, \dots, |v_n\rangle\} \sim \{|w_1\rangle, \dots, |w_n\rangle\} \Leftrightarrow \exists \theta \text{ such that } \forall j: |v_j\rangle = e^{i\theta} \cdot |w_j\rangle.$$

There is a bijective correspondence

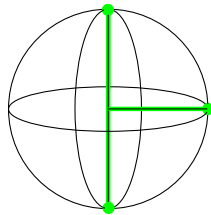
$$\mathcal{S} \begin{array}{c} \xrightarrow{sv} \\ \xleftarrow{vs} \end{array} \mathcal{V}/\sim$$

where

- $sv : \{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\} \cup \{\llbracket s \rrbracket\} \mapsto [\{\langle v_1 | s \rangle |v_1\rangle, \dots, \langle v_n | s \rangle |v_n\rangle\}]_{\sim}$
- $vs : [\{|v_1\rangle, \dots, |v_n\rangle}]_{\sim} \mapsto \{\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket\} \cup \{\llbracket \sum_i |v_i\rangle \rrbracket\}.$

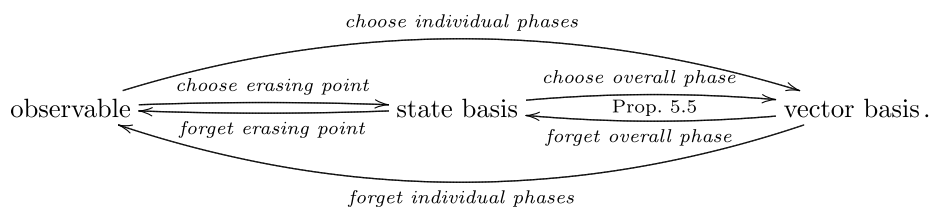
**Proof.** Note that  $sv$  is indeed well defined in the sense that its prescription does not depend on the choice of the respective vectors  $|v_1\rangle, \dots, |v_n\rangle, |s\rangle$  in the states  $\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket, \llbracket s \rrbracket$ . Also  $vs$  is easily seen to be well defined. Verifying that these maps are each other’s inverse is straightforward.  $\square$

**Example 5.6.** *On the Bloch sphere the erasing point lies on the equator for the antipodal points that represent the observable. For example, for the Z-observable  $\{\llbracket 0 \rrbracket, \llbracket 1 \rrbracket\}$  and the erasing point  $\llbracket + \rrbracket := \llbracket |0\rangle + |1\rangle \rrbracket$ , we have*



so the observable and the erasing point together make up a T-shape.

Given a vector basis, we can turn it into an observable by forgetting the phases of each of the basis vectors, which we formalize by passing to equivalence classes. To construct a vector basis from an observable, we have to choose a phase for each basis element. This construction factors over the construction of state bases as follows:



**Definition 5.7.** A pair of mutually unbiased vector bases (MUVBs),  $\mathcal{V} = \{|v_1\rangle, \dots, |v_n\rangle\}$  and  $\mathcal{W} = \{|w_1\rangle, \dots, |w_n\rangle\}$ , are called coherent iff

$$\frac{1}{\sqrt{n}} \sum_i v_i \in \mathcal{W}, \quad \frac{1}{\sqrt{n}} \sum_i w_i \in \mathcal{V}.$$

Two mutually unbiased state bases (MUSBs) are coherent iff the erasing point of each is contained in the observable of the other.

These notions of coherence coincide along the bijection of proposition 5.5:

**Proposition 5.8.** If  $\mathcal{V}$  and  $\mathcal{W}$  are coherent MUVBs, then  $vs([\mathcal{V}]_{\sim})$  and  $vs([\mathcal{W}]_{\sim})$  are coherent MUSBs, and if  $\mathcal{S}$  and  $\mathcal{T}$  are coherent MUSBs, then there exist  $\mathcal{V} \in sv(\mathcal{S})$  and  $\mathcal{W} \in sv(\mathcal{T})$  such that  $\mathcal{V}$  and  $\mathcal{W}$  are coherent MUVBs.

**Proof.** The first statement follows directly from the definition of  $vs$ . Let  $\mathcal{S} = \{[[v_1]], \dots, [[v_n]], [[w_1]]\}$  and  $\mathcal{T} = \{[[w_1]], \dots, [[w_n]], [[v_1]]\}$  be coherent MUSBs; for  $\mathcal{V} \in sv(\mathcal{S})$  and  $\mathcal{W} \in sv(\mathcal{T})$  we have  $\sum_i \mathcal{V} = \sum_i \langle v_i | w_1 \rangle |v_i\rangle = |w_1\rangle$  and  $\sum_i \mathcal{W} = |v_1\rangle$ . Hence, we obtain coherence if  $\langle w_1 | v_1 \rangle |w_1\rangle = |w_1\rangle$  and  $\langle v_1 | w_1 \rangle |v_1\rangle = |v_1\rangle$ , that is,  $\langle v_1 | w_1 \rangle = 1$ . This can be realized by choosing an appropriate overall phase for  $\mathcal{V}$  relative to  $\mathcal{W}$ .  $\square$

Pairs of observables arise from coherent bases:

**Theorem 5.9.** For each pair of MUVBs  $\{|v_1\rangle, \dots, |v_n\rangle\}$  and  $\{|w_1\rangle, \dots, |w_n\rangle\}$ , there exists a pair of coherent MUVBs  $\{|v'_1\rangle, \dots, |v'_n\rangle\}$  and  $\{|w'_1\rangle, \dots, |w'_n\rangle\}$  that induces the same observables i.e.  $[[v_i]] = [[v'_i]]$  and  $[[w_i]] = [[w'_i]]$  for all  $i$ .

**Proof.** Given a pair of MUVBs, forget all phases to obtain the corresponding pair of induced observables. Then adjoin as an erasing point to each of these a state of the other, in order to obtain coherent MUSBs. Now we can rely on proposition 5.8 to obtain coherent MUVBs that induce the same observable as the initial one.  $\square$

## 6. Algebras and observables

In the introduction of this paper, we already indicated how conceptual analysis leads to an algebraic characterization of bases and observables. Here we review this theory in technical detail. Its main purpose is a characterization of bases in the language of  $\dagger$ -SMCs—i.e. with no reference to vectors, sums, linear combinations, etc.—allowing bases to be defined in purely diagrammatic terms. As we shall also see, the diagrammatic presentation of bases admits very simple calculational rules in terms of the so-called ‘spiders’—indeed, those that play a central role in the ZX-calculus.

### 6.1. Monoids, comonoids and observable structures

Recall that a *monoid* is a triple  $(M, \bullet, 1_\bullet)$  with  $M$  a set,  $\bullet$  an associative multiplication, and  $1_\bullet \in M$  is its unit. The multiplication is a map:

$$m_\bullet : M \times M \rightarrow M :: (x, y) \mapsto x \bullet y \quad (23)$$

and we can also represent the unit as a map

$$e_{\bullet} : \mathbb{I} \rightarrow M :: \star \mapsto 1_{\bullet}, \quad (24)$$

where  $\mathbb{I} := \{\star\}$  is a singleton set. The associativity and unit laws of the monoid can now be rewritten in terms of composition of maps and the Cartesian product:

$$m_{\bullet} \circ (m_{\bullet} \times 1_M) = m_{\bullet} \circ (1_M \times m_{\bullet}), \quad (25)$$

$$m_{\bullet} \circ (e_{\bullet} \times 1_M) \simeq m_{\bullet} \circ (1_M \times e_{\bullet}) \simeq 1_M, \quad (26)$$

where  $1_M : M \rightarrow M$  is the identity map on  $M$ . Now,  $(M, m_{\bullet}, e_{\bullet})$  is *commutative* if

$$m_{\bullet} \circ \sigma_{M,M} = m_{\bullet}, \quad (27)$$

where  $\sigma_{M,M} : (x, y) \mapsto (y, x)$ .

More generally, commutative monoids can be defined *internally* in any SMC.

**Definition 6.1.** An *internal commutative monoid* in an SMC is a triple  $(M, m, e)$ , consisting of an object  $M$ , equipped with a multiplication  $m : M \otimes M \rightarrow M$ , and a unite  $e : \mathbb{I} \rightarrow M$ , satisfying

$$m \circ (m \otimes 1_M) = m \circ (1_M \otimes m), \quad (28)$$

$$m \circ (e \otimes 1_M) \circ \lambda_M = m \circ (1_M \otimes e) \circ \rho_M = 1_M, \quad (29)$$

$$m \circ \sigma_{M,M} = m. \quad (30)$$

By reversing the types and the order of composition we obtain a new concept.

**Definition 6.2.** An *internal cocommutative comonoid* in an SMC is a triple  $(X, \delta, \epsilon)$  consisting of an object  $X$  equipped with a comultiplication  $\delta : X \rightarrow X \otimes X$  and a counit  $\epsilon : X \rightarrow \mathbb{I}$ , satisfying

$$(\delta \otimes 1_X) \circ \delta = (1_X \otimes \delta) \circ \delta, \quad (31)$$

$$\lambda_X^{-1} \circ (\epsilon \otimes 1_X) \circ \delta = \rho_X^{-1} \circ (1_X \otimes \epsilon) \circ \delta = 1_X, \quad (32)$$

$$\sigma_{X,X} \circ \delta = \delta. \quad (33)$$

Note that in a  $\dagger$ -SMC each internal commutative monoid is also an internal cocommutative comonoid, for  $\delta := m^\dagger$  and  $\epsilon := e^\dagger$ , and vice versa.

Now consider a set  $X$  and let  $\delta : X \rightarrow X \times X$  be the function that *copies* entries, i.e.  $\delta :: x \mapsto (x, x)$ . Since  $\delta$  is a function it is also a relation, namely

$$\delta := \{(x, (x, x)) \mid x \in X\} \subseteq (X \times X) \times X, \quad (34)$$

and as a relation it admits a *relational converse*, obtained by exchanging the two entries in the pairs that make up that relation. The relational converse to  $\delta$ ,

$$m := \{((x, x), x) \mid x \in X\} \subseteq (X \times X) \times X, \quad (35)$$

relates pairs  $(x, x) \in X \times X$  to  $x \in X$ , while it does not relate pairs  $(x, y) \in X \times X$  for  $x \neq y$  to anything. Let  $\epsilon : X \rightarrow \mathbb{I}$  be the function that *erases* entries, i.e.  $\epsilon : x \mapsto \star$ . When conceived as a relation,  $\epsilon$  admits a relational converse

$$e := \{(\star, x) \mid x \in X\} \subseteq \mathbb{I} \times X, \quad (36)$$

which now relates  $\star \in \mathbb{I}$  to each  $x \in X$ . The copying/erasing pair  $(\delta, \epsilon)$  is a comonoid in **Rel**, and the pair  $(m, e)$  consisting of their respective converses is a monoid in **Rel**. The pair  $(m, \delta)$  moreover satisfies another remarkable property:

$$\delta \circ m = (1_X \times m) \circ (\delta \times 1_X) = \{(x, x), (x, x) \mid x \in X\}. \tag{37}$$

**Remark 6.3.** *This interesting property first appeared in the literature as part of Carboni and Walters’ axiomatization of the category **Rel** in [12], where they introduced the notion of a Frobenius algebra in an SMC  $\mathcal{C}$ , as a quintuple of morphisms*

$$(X, d: X \otimes X \rightarrow X, e: I \rightarrow X, \delta: X \rightarrow X \otimes X, \epsilon: X \rightarrow I), \tag{38}$$

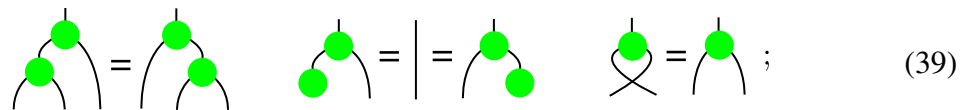
where  $(X, m, e)$  is an internal commutative monoid and  $(X, \delta, \epsilon)$  is an internal cocommutative comonoid, which together satisfy the Frobenius law— see (40) below.

**Definition 6.4.** [27] *An observable structure in a  $\dagger$ -SMC is a triple*

$$(A, \delta = \text{green dot with two outgoing wires} : A \rightarrow A \otimes A, \epsilon = \text{green dot with one outgoing wire} : A \rightarrow I),$$

which

(i) *is a cocommutative comonoid; the defining equations (31)–(33) are depicted as:*



$$\tag{39}$$

(ii) *satisfies the Frobenius law, i.e.*

$$(\delta^\dagger \otimes 1_A) \circ (1_A \otimes \delta) = \delta \circ \delta^\dagger, \text{ i.e. } \text{green dot with two wires} = \text{green dot with two wires}; \tag{40}$$

(iii) *is special, i.e.*

$$\delta^\dagger \circ \delta = 1_A \text{ i.e. } \text{green dot with one wire and a loop} = \text{vertical line}. \tag{41}$$

**Example 6.5.** *The unit object  $I$  canonically comes with an observable structure:*

$$\delta_I := \lambda_I : I \simeq I \otimes I \quad \epsilon_I := 1_I. \tag{42}$$

**Example 6.6.** *As indicated in the introduction to this paper, any orthonormal basis  $\{|\psi_i\rangle\}_i$  for a Hilbert space  $\mathcal{H}$  induces an observable structure by considering the linear maps that respectively ‘copy’ and ‘uniformly erase’ the basis vectors:*

$$\delta : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H} :: |\psi_i\rangle \mapsto |\psi_i\rangle \otimes |\psi_i\rangle, \quad \epsilon : \mathcal{H} \rightarrow \mathbb{C} :: |\psi_i\rangle \mapsto 1. \tag{43}$$

Moreover, this observable structure is ‘basis capturing’: we can recover the basis vectors from which we constructed  $\delta$  as the solutions to the equation

$$\delta(|\psi\rangle) = |\psi\rangle \otimes |\psi\rangle. \tag{44}$$

This also shows that the basis  $\{|\psi_i\rangle\}_i$  is faithfully encoded in the linear map  $\delta$  alone and that  $\epsilon$  does not carry any additional data.

Conversely, all observable structures in **FdHilb** arise from bases:

**Theorem 6.7.** [28] *All observable structures in **FdHilb** are of the form (43).*

So observable structures provide an *axiomatic characterization* of bases in  $\dagger$ -SMC language, with no reference to the linear structure of the underlying vector spaces.

**Example 6.8.** *Each observable structure in **FdHilb** induces an observable structure in **FdHilb**<sub>wp</sub> in an obvious manner. But in the light of proposition 5.5, the correspondence in **FdHilb** between observable structures and vector bases becomes one between observable structures and state bases in **FdHilb**<sub>wp</sub>. Note that*

$$\delta : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H} :: \llbracket |\psi_i\rangle \rrbracket \mapsto \llbracket |\psi_i\rangle \otimes |\psi_i\rangle \rrbracket \tag{45}$$

does not define a unique  $\delta$  anymore. In addition, we need to specify that  $\llbracket \left[ \sum_i |\psi_i\rangle \right] \rrbracket$ , the erasing point of the state basis, provides the unit for the comultiplication:

$$\delta^\dagger \left( - \otimes \left[ \left[ \sum_i |\psi_i\rangle \right] \right] \right) = 1_{\mathcal{H}}. \tag{46}$$

**Corollary 6.9.** *Observable structures in **FdHilb**<sub>wp</sub> are in bijective correspondence with state bases via the correspondence outlined in example 6.8.*

**Example 6.10.** *The somewhat surprising fact that there are observable structures in **FRel** other than those of the form (35), (36) was noted by Edwards and one of the authors in [19]. The observable structures in **FRel** have been classified by Pavlovic in [60], in terms of groups. The notion of observable structure also applies to non-standard quantum-like theories. For example, it provides a generalized notion of basis for Spekkens’ toy theory [19], despite the lack of an underlying vector space structure.*

When the monoidal structure is strict, which is always the case in the graphical language, observable structures obey the following remarkable theorem, which follows from results in [53, 54]—a direct derivation is given in [23].

**Theorem 6.11** (normal form). *Let  $\delta_n : A \rightarrow A^{\otimes n}$  be defined by the recursion*

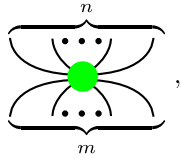
$$\delta_0 = \epsilon, \quad \delta_n = (\delta_{n-1} \otimes 1_A) \circ \delta, \quad \text{i.e.} \quad \text{[Diagram: A node with } n \text{ inputs and } n \text{ outputs, representing } \delta_n \text{]} \tag{47}$$

If  $f : A^{\otimes n} \rightarrow A^{\otimes m}$  is a morphism generated from the observable structure  $(A, \delta, \epsilon)$ , the symmetric monoidal structure maps, and the adjoints of all of these, and if the graphical representation of  $f$  is connected, then we have

$$f = \delta_m \circ \delta_n^\dagger, \quad \text{i.e.} \quad \text{[Diagram: A node with } m \text{ inputs and } n \text{ outputs, representing } f \text{]} \tag{48}$$

Hence,  $f$  only depends on the object  $A$  and the number of inputs  $n$  and outputs  $m$ .

**Theorem 6.12** (spider rules). *When representing the unique morphism with  $n$  inputs and  $m$  outputs of theorem 6.11 as an ‘ $n + m$ -legged spider’:*



then these spiders obey the following composition rule:

(49)

i.e. when two spiders ‘share legs’ then these two spiders ‘fuse’ into a single spider. Also, the  $1 + 1$ -legged spider must be equal to the identity:

(50)

and thirdly, spiders are invariant under ‘leg swapping’:

(51)

Conversely, given a family  $\{\delta_m^\dagger \circ \delta_n | n, m \in \mathbb{N}\}$  of morphisms, the equations defining an observable structure can be recovered from (49), (50) and (51), hence providing an alternative characterization of observable structures now purely in terms of spiders.

**Example 6.13.** *We have*

$$(1_A \otimes \delta_2^\dagger) \circ (\delta_2 \otimes \delta_2) \circ (1_A \otimes \sigma_{A,A} \otimes 1_A) \circ (\delta_2^\dagger \otimes \delta_2^\dagger) \circ (\delta_2 \otimes 1_A)$$

The spider rules enabled us to define the ZX-calculus of section 2 in terms of spiders obeying rules (49) and (50), rather than algebras. The swapping of remaining rule (51) was eliminated by (implicitly) allowing freedom of how to spiders may be connected, absorbing the symmetry into the graph structure (see example 2.3). Here we have been more explicit. The angles labelling the spiders of the ZX-calculus will be explained below in section 7.



6.2. Induced  $\dagger$ -compact structure

**Definition 6.14.** A self-dual  $\dagger$ -compact structure is a pair

$$(A, \eta : I \rightarrow A \otimes A)$$

which satisfies equations (21) and (22).

**Proposition 6.15.** Every observable structure on an object  $A$  defines a self-dual  $\dagger$ -compact structure when setting  $\eta = \delta_2^0$ .

**Proof.** Equations (21) and (22) follow from equations (49) and (51), respectively. □

**Remark 6.16.** The  $\dagger$ -compact structures induced by different observable structures may or may not coincide [26]. For example, while  $\dagger$ -compact structures induced by the observable structures that copy the  $\{|0\rangle, |1\rangle\}$  and  $\{|+\rangle, |-\rangle\}$  coincide, this is not the case for the bases  $\{|0\rangle, |1\rangle\}$  and  $\{|0\rangle + i|1\rangle, |0\rangle - i|1\rangle\}$ . Returning to the ZX-calculus, the two equations of the S2-rule are quite different from each other. The equations

$$\begin{array}{c} | \\ \bullet \\ | \end{array} = \begin{array}{c} | \\ | \\ | \end{array} = \begin{array}{c} | \\ \bullet \\ | \end{array}$$

are true because of the counit law for the observable structure, and the fact that there is only one identity map. On the other hand, the equations

$$\begin{array}{c} \bullet \\ \cup \end{array} = \begin{array}{c} \bullet \\ \cup \end{array} \quad \begin{array}{c} \cup \\ \bullet \end{array} = \begin{array}{c} \cup \\ \bullet \end{array}$$

are not a consequence of the axioms of an observable structure, but a fact specific to the Z- and X-bases. Only when no confusion is possible do we simplify the notation for the 0+2-legged spider, as in the ZX-calculus:

$$\begin{array}{c} \bullet \\ \cup \end{array} = \cup$$

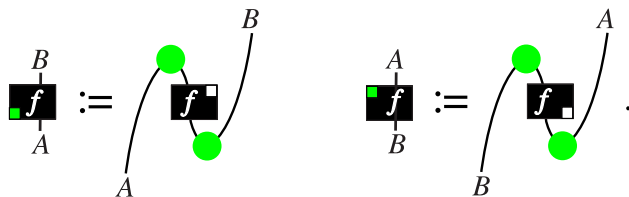
The dots will be retained when disambiguation is required.

**Definition 6.17.** Let  $f : A \rightarrow B$  be a morphism. Its transpose,  $f^* : B \rightarrow A$ , and its conjugate,  $f_* : A \rightarrow B$ , relative to observables structures on  $A$  and  $B$ , are defined as

$$f^* := (1_A \otimes \eta_B^\dagger) \circ (1_A \otimes f \otimes 1_B) \circ (\eta_A \otimes 1_B),$$

$$f_* := (1_B \otimes \eta_A^\dagger) \circ (1_B \otimes f^\dagger \otimes 1_A) \circ (\eta_B \otimes 1_A).$$

Diagrammatically, we denote  $f^*$  and  $f_*$ , respectively, as



The green squares indicate the dependence of  $f^*$  and  $f_*$  on the observable structures on  $A$  and  $B$ ; when there is no risk of confusion we omit the colouration and rely simply on the position

of the indicated corner to distinguish between  $f$ ,  $f^\dagger$ ,  $f^*$  and  $f_*$ . We follow [68] in representing the conjugate by horizontal reflection and the transpose by a 180° rotation:

$$\begin{array}{c|c}
 f = \begin{array}{c} A \\ \boxed{f} \\ B \end{array} & f_* = \begin{array}{c} A \\ \boxed{f} \\ B \end{array} \\
 \hline
 f^\dagger = \begin{array}{c} B \\ \boxed{f} \\ A \end{array} & f^* = \begin{array}{c} B \\ \boxed{f} \\ A \end{array}
 \end{array}$$

which is consistent with the fact that

$$f_* = (f^\dagger)^* = (f^*)^\dagger, \quad \text{or equivalently,} \quad f^\dagger = (f_*)^* = (f^*)_*.$$

**Corollary 6.18.** *For an observable structure, all spiders are self-conjugate.*

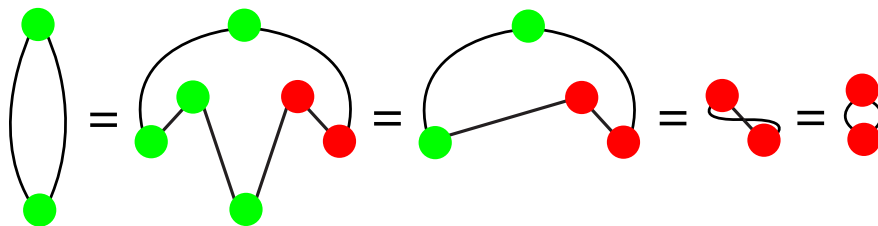
**Example 6.19.** *In  $\mathbf{FdHilb}$ , every observable structure corresponds to a basis, as per example 6.6. The linear function  $f_*$  is obtained by conjugating the entries of the matrix of  $f$  when expressed in the bases corresponding to the observable structures on  $A$  and  $B$ ;  $f^*$  is obtained by transposing the matrix of  $f$ .*

**Definition 6.20.** *Let  $A$  be an object in a  $\dagger$ -SMC which comes with an observable structure, and hence an induced  $\dagger$ -compact structure  $(A, \eta)$ . The dimension of  $A$  is  $\dim(A) := \eta^\dagger \circ \eta$ , represented graphically by a circle:*

$$\bigcirc := \begin{array}{c} \bullet \\ \bullet \end{array}$$

**Lemma 6.21.** *Dimension is independent of the choice of observable structure.*

**Proof.** We will depict the two distinct observable structures in green and red, respectively. Then, repeatedly relying on  $\dagger$ -compactness, we have



so the circles induced by the two observable structures coincide. □

**Remark 6.22.** *In the language of  $\dagger$ -compact categories, the circle is formed by taking the trace of the identity morphism; in a finite dimensional Hilbert space this will always give the dimension, hence the terminology  $\dim A$ .*

6.3. Classical points and generalized bases

We now provide a category-theoretic counterpart to the role played by basis vectors/states in  $\mathbf{FdHilb}$  and  $\mathbf{FdHilb}_{wp}$ .

**Definition 6.23.** Given an observable structure  $(A, \delta, \epsilon)$ , a morphism  $k: I \rightarrow A$  is a classical point iff it is a self-conjugate comonoid homomorphism, that is, graphically:

$$\begin{array}{c} \textcircled{k} \\ \downarrow \end{array} = \begin{array}{c} \textcircled{k} \\ \downarrow \end{array} \tag{52}$$

$$\begin{array}{c} \textcircled{k} \\ \downarrow \\ \bullet \end{array} = \begin{array}{c} \textcircled{k} \quad \textcircled{k} \\ \downarrow \quad \downarrow \\ \bullet \end{array} \tag{53}$$

$$\begin{array}{c} \textcircled{k} \\ \downarrow \\ \bullet \end{array} = \begin{array}{c} \bullet \end{array} \tag{54}$$

**Remark 6.24.** The notation  $\begin{array}{c} \textcircled{k} \\ \downarrow \end{array}$  reflects ‘sensitivity to conjugation’, while the notation  $\begin{array}{c} \textcircled{k} \\ \downarrow \\ \bullet \end{array}$  reflects ‘invariance under conjugation’. We used  $\begin{array}{c} \textcircled{k} \\ \downarrow \end{array}$  in (52) to express invariance under conjugation, and given this fact, we used  $\begin{array}{c} \textcircled{k} \\ \downarrow \\ \bullet \end{array}$  in (53) and (54).

**Proposition 6.25.** Classical points are normalized.

**Proof.** Since each classical point  $k: I \rightarrow A$  is self-conjugate its adjoint  $k^\dagger: A \rightarrow I$  and its transpose  $k^*: A \rightarrow I$  coincide. Hence we have

$$\begin{array}{c} \textcircled{k} \\ \downarrow \\ \textcircled{k} \end{array} = \begin{array}{c} \textcircled{k} \quad \textcircled{k} \\ \downarrow \quad \downarrow \\ \cup \end{array} = \begin{array}{c} \textcircled{k} \\ \downarrow \\ \cup \end{array} = \begin{array}{c} \textcircled{k} \\ \downarrow \\ \bullet \end{array} = \begin{array}{c} \bullet \end{array}$$

i.e.  $k^\dagger \circ k = 1_I$ . □

**Example 6.26.** In  $\mathbf{FdHilb}$  the classical points for an observable structure are exactly the basis vectors  $\{|v_1\rangle, \dots, |v_n\rangle\}$  and in  $\mathbf{FdHilb}_{wp}$  they constitute the corresponding observable  $\{|v_1\rangle, \dots, |v_n\rangle\}$ . Hence, while in  $\mathbf{FdHilb}$  the classical points completely determine an observable structure, this is not the case in  $\mathbf{FdHilb}_{wp}$ , where it is the classical points together with an erasing point that determine an observable structure.

The following is a category-theoretic generalization of a notion of basis, either in the sense of proposition 5.2 or in the sense of proposition 5.4, which, respectively, applies to the categories  $\mathbf{FdHilb}$  and  $\mathbf{FdHilb}_{wp}$ .

**Definition 6.27.** An observable structure  $(A, \delta, \epsilon)$  with classical points  $\mathcal{K}$  is called a vector basis iff for all objects  $B$  and all morphisms  $f, g: A \rightarrow B$ , we have

$$[\forall k \in \mathcal{K} : f \circ k = g \circ k] \Rightarrow f = g. \tag{55}$$

It is called a state basis iff for all  $B$  and all  $f, g: A \rightarrow B$ , we have

$$[\forall k \in \mathcal{K} \cup \{\epsilon^\dagger\} : f \circ k = g \circ k] \Rightarrow f = g. \tag{56}$$

One can easily construct new observable structures by combining old ones, as in the following proposition.

**Proposition 6.28.** *Two observable structures  $(A, \delta_A, \epsilon_A)$  and  $(B, \delta_B, \epsilon_B)$  canonically induce an observable structure on  $A \otimes B$  with*

$$\delta_{A \otimes B} = (1_A \otimes \sigma_{A,B} \otimes 1_B) \circ (\delta_A \otimes \delta_B) \quad \text{i.e.} \quad \begin{array}{c} \text{A} \quad \text{B} \\ | \quad | \\ \text{---} \text{---} \\ | \quad | \end{array}, \quad (57)$$

and

$$\epsilon_{A \otimes B} = \lambda_I^\dagger \circ (\epsilon_A \otimes \epsilon_B) \quad \text{i.e.} \quad \begin{array}{c} \text{A} \quad \text{B} \\ | \quad | \\ \text{---} \end{array}. \quad (58)$$

Moreover, if  $k : I \rightarrow A$  is a classical point for  $(A, \delta_A, \epsilon_A)$  and  $k' : I \rightarrow B$  is a classical point for  $(B, \delta_B, \epsilon_B)$ , then  $(k \otimes k') \circ \lambda_I$  is a classical point for  $(A \otimes B, \delta_{A \otimes B}, \epsilon_{A \otimes B})$ .

**Definition 6.29.** *We say that the monoidal tensor lifts vector bases iff for all vector bases  $(A, \delta_A, \epsilon_A)$  with classical points  $\mathcal{K}$  and  $(B, \delta_B, \epsilon_B)$  with classical points  $\mathcal{K}'$ , all objects  $C$ , and all morphisms  $f, g : A \otimes B \rightarrow C$ , we have that*

$$[\forall (k, k') \in \mathcal{K} \times \mathcal{K}' : f \circ (k \otimes k') = g \circ (k \otimes k')] \Rightarrow f = g. \quad (59)$$

– hence it follows that the observable structure  $(A \otimes B, \delta_{A \otimes B}, \epsilon_{A \otimes B})$  is also vector basis. Similarly, the monoidal tensor lifts state bases iff

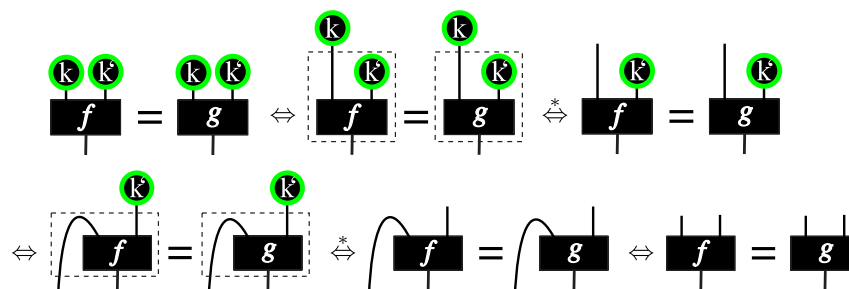
$$[\forall (k, k') \in (\mathcal{K} \times \mathcal{K}') \cup \{(\epsilon_A^\dagger, \epsilon_B^\dagger)\} : f \circ (k \otimes k') = g \circ (k \otimes k')] \Rightarrow f = g. \quad (60)$$

– hence it follows that  $(A \otimes B, \delta_{A \otimes B}, \epsilon_{A \otimes B})$  is also state basis.

Since observable structures induce  $\dagger$ -compact structures we have the following.

**Proposition 6.30.** *Monoidal tensors always lift vector bases and state bases.*

**Proof.** We have



where the marked equivalences rely on the vector/state basis assumption. □

### 7. Phase shifts and a generalized spider theorem

In the preceding section, we saw that observable structures correspond to bases of our state space; now we introduce an abstract notion of *phase* relative to a given basis, and generalize theorems 6.11 and 6.12 to incorporate such phase shifts.

7.1. A monoid structure on points

**Definition 7.1.** Let  $(A, \delta, \epsilon)$  be an observable structure in a  $\dagger$ -SMC  $\mathcal{C}$  and let  $\mathbf{C}(I, A)$  be the underlying set of points. We define a multiplication on points

$$- \circ - : \mathbf{C}(I, A) \times \mathbf{C}(I, A) \rightarrow \mathbf{C}(I, A) \tag{61}$$

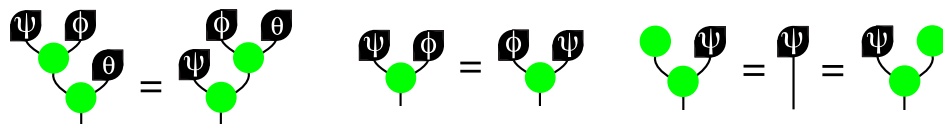
by setting, for all points  $\psi, \phi \in \mathbf{C}(I, A)$ ,

$$\psi \circ \phi := \delta^\dagger \circ (\psi \otimes \phi) \circ \lambda_I \quad \text{i.e.} \quad \text{Diagram} = \text{Diagram} \tag{62}$$

**Remark 7.2.** As already explained in remark 6.24, the shape of the points reflects that they may not be invariant under conjugation.

**Proposition 7.3.**  $(\mathbf{C}(I, A), \circ, \epsilon^\dagger, (-)_*)$  is an involutive commutative monoid.

**Proof.** Associativity, commutativity and that  $\epsilon^\dagger$  is the monoid’s unit, i.e.



follow immediately from internal monoid laws for  $(A, \delta^\dagger, \epsilon^\dagger)$ —see (39) above—and conjugation is an involution since  $\delta^\dagger$  is self-conjugate—see corollary 6.18.  $\square$

**Example 7.4.** Let  $\delta_Z : \mathbb{C}^2 \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$  be defined by  $\delta : |i\rangle \mapsto |ii\rangle$ . The induced multiplication  $\circ_Z$  is just point-wise multiplication in the standard basis:

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ_Z \begin{pmatrix} a' \\ b' \end{pmatrix} = \delta_Z^\dagger \left( \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} a' \\ b' \end{pmatrix} \right) = \begin{pmatrix} aa' \\ bb' \end{pmatrix}.$$

Indeed, the same will be true for any observable structure, provided we write the vectors in the corresponding basis.

As well as giving an involutive commutative monoid on the points of  $A$ , we can use  $\delta^\dagger$  to lift this monoid up to the endomorphisms of  $A$ .

**Definition 7.5.** For  $(A, \delta, \epsilon)$  an observable structure in a  $\dagger$ -SMC  $\mathcal{C}$ , let

$$\Lambda : \mathbf{C}(I, A) \rightarrow \mathbf{C}(A, A) \tag{63}$$

be defined by setting, for each point  $\psi \in \mathbf{C}(I, A)$ ,

$$\Lambda(\psi) = \delta^\dagger \circ (\psi \otimes 1_A) \quad \text{i.e.} \quad \text{Diagram} = \text{Diagram}, \tag{64}$$

and we denote the range of  $\Lambda$  by  $\Lambda(A, A)$ .

**Proposition 7.6.** *The map  $\Lambda$  is an isomorphism of involutive commutative monoids:*

$$(\mathbf{C}(\mathbf{I}, A), \odot, \epsilon^\dagger, (-)_*) \simeq (\Lambda(A, A), \circ, 1_A, (-)^\dagger), \tag{65}$$

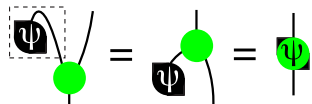
that is, explicitly:

$$\Lambda(\psi \odot \phi) = \Lambda(\psi) \circ \Lambda(\phi), \quad \Lambda(\epsilon^\dagger) = 1_A, \quad \Lambda(\psi_*) = \Lambda(\psi)^\dagger, \tag{66}$$

and hence commutativity is inherited:

$$\Lambda(\psi) \circ \Lambda(\phi) = \Lambda(\psi \odot \phi) = \Lambda(\phi \odot \psi) = \Lambda(\phi) \circ \Lambda(\psi) \quad \text{i.e.} \quad \begin{array}{c} \Psi \\ \Phi \end{array} = \begin{array}{c} \Psi \odot \Phi \\ \Phi \end{array} = \begin{array}{c} \Phi \\ \Psi \end{array}. \tag{67}$$

**Proof.** Preservation of monoid multiplication and unit follows directly from the unit and commutativity law of the internal monoid. By the spider rules, we have

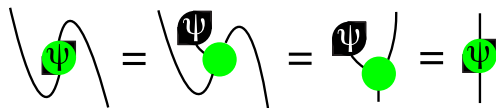


that is, conjugation of points is mapped to the adjoint of endomorphisms. □

Note that the notation of endomorphisms in  $\Lambda(A, A)$  is invariant under 180° rotation. This is justified by the following proposition.

**Proposition 7.7.** *Each  $\Lambda(\psi) \in \Lambda(A, A)$  is equal to its transpose.*

**Proof.** We have



where we have relied on the spider rules. □

**Proposition 7.8.** *The endomorphisms in  $\Lambda(A, A)$  obey*

$$\Lambda(\psi) \circ \delta^\dagger = \delta^\dagger \circ (1_A \otimes \Lambda(\psi)) = \delta^\dagger \circ (\Lambda(\psi) \otimes 1_A), \tag{68}$$

i.e.

$$\begin{array}{c} \Psi \\ \Psi \end{array} = \begin{array}{c} \Psi \\ \Psi \end{array} = \begin{array}{c} \Psi \\ \Psi \end{array}, \tag{69}$$

**Proof.** By the spider rules, all three diagrams normalize to



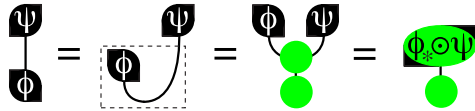
so they are all indeed equal. □

The following proposition shows that the inner-product structure on points is subsumed by the commutative involutive monoid structure on points.

**Proposition 7.9.** For points  $\psi, \phi : I \rightarrow A$  in  $\mathcal{C}$  we have

$$\langle \phi | \psi \rangle := \phi^\dagger \circ \psi = \epsilon \circ (\phi_* \odot \psi). \tag{70}$$

**Proof.** Using the definition of the transpose for  $\phi^\dagger = (\phi_*)^*$  we obtain



where again we used the spider rules. □

### 7.2. The decorated spider theorem

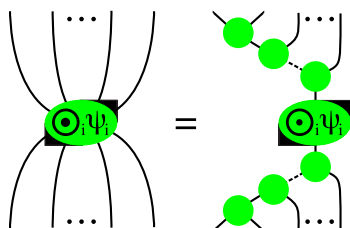
**Theorem 7.10 (normal form with points).** If  $f : A^{\otimes n} \rightarrow A^{\otimes m}$  is a morphism generated from the observable structure  $(A, \delta, \epsilon)$ , the symmetric monoidal structure maps, and the adjoints of all of these, points  $\psi_i : I \rightarrow A$  (exactly one occurrence for each  $i$ ), and if the graphical representation of  $f$  is connected, then we have

$$f = \delta_m \circ \Lambda(\odot_i \psi_i) \circ \delta_n^\dagger, \quad \text{i.e.} \quad \begin{array}{c} \overbrace{\dots}^n \\ \vdots \\ \odot_i \psi_i \\ \vdots \\ \underbrace{\dots}_m \end{array}$$

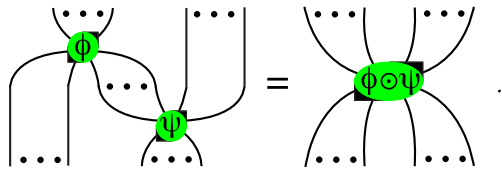
**Proof.** If neither  $\delta$  nor  $\delta^\dagger$  occurs in  $f$ , then the result is trivial. Otherwise, all points  $\psi_i$  occurring in  $f$  may be lifted to  $\Lambda(\psi_i)$ ; by virtue of proposition 7.8, these commute freely with the observable structure, and hence can all be collected together. The result now follows by applying theorem 6.11. □

Theorem 7.10 is a strict generalization of theorem 6.11: diagrams with equal numbers of inputs  $n$  and outputs  $m$  are equal whenever the product of points occurring in them is also equal. The theorem gives a specific normal form to which this entire class of diagrams is equal; we also have corresponding *decorated spider rules*.

**Theorem 7.11** (decorated spider rules). When setting



these decorated spiders obey the following composition rule:



i.e. if two decorated spiders ‘share legs’, then these two spiders ‘fuse’ together into a single decorated spider provided we ‘multiply decorations’.

This is of course the form of the spider rule in the ZX-calculus.

### 7.3. Unbiased points

**Example 7.12.** Let  $(\delta, \epsilon)$  be the observable structure corresponding to the standard basis of  $\mathbb{C}^n$ , and consider  $|\psi\rangle = \sum_i c_i |i\rangle$ . When written in the basis fixed by  $(\delta, \epsilon)$ ,  $\Lambda(\psi)$  consists of the diagonal  $n \times n$  matrix with  $c_1, \dots, c_n$  on the diagonal. Hence,  $\Lambda(\psi)$  is unitary if and only if  $\bar{c}_1 c_1 = \dots = \bar{c}_n c_n = 1$ , that is, if and only if  $|\psi\rangle$  is unbiased for  $\{|1\rangle, \dots, |n\rangle\}$  (up to a normalizing constant).

This situation admits generalization to arbitrary  $\dagger$ -SMCs.

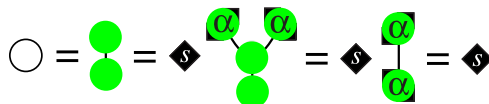
**Definition 7.13.** We call a point  $\alpha : I \rightarrow A$  unbiased relative to an observable structure  $(A, \delta, \epsilon)$  if there exists a scalar  $s : I \rightarrow I$  such that

$$s \cdot \alpha \odot \alpha_* = \epsilon^\dagger, \quad \text{i.e.} \quad \begin{array}{c} \alpha \quad \alpha \\ \diagdown \quad / \\ \bullet \\ \diagup \quad \diagdown \\ s \end{array} = \begin{array}{c} \bullet \\ | \\ s \end{array} \quad (71)$$

**Example 7.14.** Since by the spider rules the point  $\epsilon^\dagger$  satisfies this definition, every observable structure has at least one unbiased point, namely its unit.

**Lemma 7.15.** If an unbiased point  $\alpha$  is normalized, i.e.  $\alpha^\dagger \circ \alpha = 1_I$ , then the scalar  $s$  in the above definition is equal to  $D = \dim A$ . Hence, if on the other hand  $|\alpha|^2 := \alpha^\dagger \circ \alpha = D$ , then this scalar is  $1_I$ .

**Proof.** We have



where we have relied on proposition 7.9. □

The expression  $\alpha \odot \alpha_*$  denotes ‘convolution’ of  $\alpha$  with itself; since the point  $\epsilon^\dagger$  represents the uniform distribution over the basis defining  $\delta$ , this definition indeed captures the usual understanding of what it means for a vector to be unbiased with respect to a basis. The following shows that this is exactly correct.



**Lemma 7.16.** *Let  $\alpha, k : I \rightarrow A$  be points of  $A$  such that  $\alpha$  is unbiased and normalized, and  $k$  is classical, for  $(A, \delta, \epsilon)$ ; then*

$$D \cdot |\langle k | \alpha \rangle|^2 := D \cdot (k^\dagger \circ \alpha) \cdot (\alpha^\dagger \circ k) = 1_I \quad \text{i.e.} \quad \bigcirc \begin{array}{c} \alpha \quad k \\ | \\ k \quad \alpha \end{array} = \quad . \quad (72)$$

**Proof.** We have

$$\bigcirc \begin{array}{c} \alpha \quad k \\ | \\ k \quad \alpha \end{array} = \bigcirc \begin{array}{c} k \quad k \\ | \\ \alpha \quad \alpha \end{array} = \bigcirc \begin{array}{c} k \\ / \quad \backslash \\ \alpha \quad \alpha \end{array} = \begin{array}{c} k \\ | \\ \bullet \end{array} =$$

where we relied on the fact that scalars are always self-transpose, used (53), used the adjoint to the unbiasedness law and finally used (54).  $\square$

**Remark 7.17.** *To retrieve the usual definition of unbiasedness,*

$$|\langle z | \alpha \rangle| = \frac{1}{\sqrt{\dim A}}, \quad (73)$$

*we simply divide; however, since we operate in an arbitrary  $\dagger$ -SMC, the scalars form a commutative monoid rather than a group, so dividing is not always possible. Hence the form (72) for the unbiasedness law.*

#### 7.4. The phase group

**Proposition 7.18.** *A point  $\alpha$  of length  $|\alpha|^2 = D$  is unbiased iff  $\Lambda(\alpha)$  is unitary.*

**Proof.** Due the commutativity property of  $\Lambda$  in proposition 7.6, we need check only one equation to show that  $\Lambda(\alpha)$  is unitary, namely,

$$\Lambda(\alpha) \circ \Lambda(\alpha)^\dagger = 1_A, \quad \text{i.e.} \quad \begin{array}{c} \alpha \\ | \\ \alpha \end{array} = \left| \quad . \quad (74)$$

Suppose that  $\alpha$  is unbiased; then, by the spider rules, we have

$$\begin{array}{c} \alpha \\ | \\ \alpha \end{array} = \begin{array}{c} \alpha \quad \alpha \\ / \quad \backslash \\ \bullet \quad \bullet \\ \backslash \quad / \\ \bullet \end{array} = \begin{array}{c} \bullet \\ / \quad \backslash \\ \bullet \quad \bullet \end{array} = \left| \quad ,$$

as required. The other direction of the proof is essentially the same.  $\square$

Since unitary maps are invertible, they form a group, and this group structure transfers back onto the unbiased points.

**Theorem 7.19.** *If in the isomorphism of involutive commutative monoids of proposition 7.6 we restrict ourselves to unbiased points relative to the observable structure of length  $|\alpha|^2 = D$ , and unitary endomorphisms, then we obtain an isomorphism of Abelian groups, with the involution as the inverse.*

**Proof.** This immediately follows from proposition 7.18 and the fact that for a unitary morphism the adjoint is the inverse.  $\square$

**Definition 7.20.** The Abelian group of endomorphisms of theorem 7.19 is called the phase group, and its elements are called phase shifts.

**Remark 7.21.** We chose  $|\alpha|^2 = D$  since this results in the inverse taking a simple form; fixing another length would also have given us an Abelian group structure.

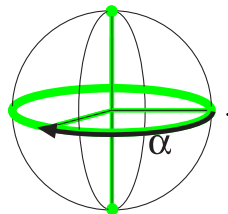
**Example 7.22.** Consider the observable structure  $(\mathbb{C}^2, \delta_Z, \epsilon_Z)$  in **FdHilb**, defined by

$$\delta_Z : |i\rangle \mapsto |ii\rangle, \quad \epsilon_Z : |0\rangle + |1\rangle \mapsto 1.$$

Its classical points are  $\{|0\rangle, |1\rangle\}$ . The unbiased points for  $(\mathbb{C}^2, \delta_Z, \epsilon_Z)$  are of the form  $|\alpha_Z\rangle = |0\rangle + e^{i\alpha}|1\rangle$ , and  $|\alpha_Z\rangle \odot_Z |\beta_Z\rangle = |(\alpha + \beta)_Z\rangle$ ; hence the group of unbiased points is isomorphic to the interval  $[0, 2\pi)$  under addition modulo  $2\pi$ . We have

$$\Lambda^Z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix},$$

and in particular,  $\Lambda^Z(\pi) = Z$ . In other words, the phase shifts of the observable structure are obtained by rotating along the equator of the Bloch sphere:



In particular, we have  $|\theta_1\rangle \odot |\theta_2\rangle = |\theta_1 + \theta_2\rangle$ , i.e. the operation  $\odot$  is simply addition modulo  $2\pi$ , which is an Abelian group with minus as inverse. This group of phases played a key role in proving universality of the ZX-calculus in section 2.4.

**Example 7.23.** Phase groups can provide an algebraic witness for physical differences between theories. For example, as shown in [20], the toy model category **Spek** (cf example 4.20) and the category **Stab** (a restriction of **FdHilb** to the qubit stabilizer states) are essentially the same except for the phase groups of their respective qubits. In the case of **Spek** the phase group is the Klein four group  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , whereas for **Stab** the phase group is the cyclic four group  $\mathbb{Z}_4$ . This difference in phase groups is closely connected with the fact that while states in **Spek** always admit a local hidden variable representation, in **Stab** there are states that do not, namely the GHZ state [58].

**Example 7.24.** Using decorated spider notation, we can set

$$\begin{array}{c} \alpha \\ \diagup \quad \diagdown \\ \square \end{array} := (\Lambda(\alpha) \otimes \Lambda(\alpha)) \circ \delta \circ \Lambda(\alpha)^\dagger \quad \text{and} \quad \begin{array}{c} \alpha \\ \diagdown \quad \diagup \\ \square \end{array} := \epsilon \circ \Lambda(\alpha)^\dagger,$$

and for  $\alpha$  unbiased relative to  $(A, \delta, \epsilon)$ , again by the decorated spider rules, it follows that these morphisms define an observable structure. Hence, each element of the phase group transforms the given observable structure into a new observable structure.

## 8. Complementarity is equivalent to the Hopf law

For observable structures  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  in a  $\dagger$ -SMC, we will denote the corresponding induced  $\dagger$ -compact structures respectively as  $(A, \eta_Z)$  and  $(A, \eta_X)$ . First we study complementarity for pairs of observable structures on the same object with coinciding induced  $\dagger$ -compact structures, and then we study the slightly more involved case of non-coinciding induced  $\dagger$ -compact structures— cf remark 6.16.

### 8.1. Observable structures with coinciding $\dagger$ -compact structures

First we define complementarity for observable structures in arbitrary  $\dagger$ -SMCs in a manner that makes explicit reference to their classical points, simply in analogy to the usual definition in the Hilbert space quantum theory, and then we show that this definition can be equivalently restated without any reference to points.

**Definition 8.1.** *Two observable structures  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  in a  $\dagger$ -SMC are called complementary if they obey the following rules:*

- **comp1** whenever  $z : I \rightarrow A$  is classical for  $(\delta_Z, \epsilon_Z)$  it is unbiased for  $(\delta_X, \epsilon_X)$ ;
- **comp2** whenever  $x : I \rightarrow A$  is classical for  $(\delta_X, \epsilon_X)$  it is unbiased for  $(\delta_Z, \epsilon_Z)$ .

We abbreviate *complementary observable structures* as COS.

*Notation.* Graphically we distinguish two distinct observable structures in terms of their colour. To emphasize that a classical point  $k : I \rightarrow A$  is copied by an observable structure of one colour, say green, whereas it is unbiased with respect to an observable structure of another colour, say red, we denote them by



that is, the outside colour indicates which observable structure copies this point, whereas the inner colour shows to which observable structure the point is unbiased.

The fact that we denote these points in a manner that is invariant under conjugation is a consequence of the trivial observation that classical points of one colour are not only self-conjugate for ‘their own colour’ (cf corollary 6.18), but also self-conjugate for ‘another colour’ provided induced  $\dagger$ -compact structures coincide:

**Proposition 8.2.** *If  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  are observable structures with*

$$\eta_Z = \eta_X, \quad \text{i.e.} \quad \text{green } \text{hook} = \text{red } \text{hook}, \quad (75)$$

*then for classical points  $k : I \rightarrow A$  of  $(\delta_Z, \epsilon_Z)$  and  $k' : I \rightarrow A$  of  $(\delta_X, \epsilon_X)$ , we have*

$$k = k_{*X} = (k^\dagger \otimes 1_A) \circ \eta_X, \quad \text{i.e.} \quad \text{green } \text{circle with red dot} = \text{red } \text{circle with green dot}, \quad (76)$$

$$k' = k'_{*Z} = (k'^\dagger \otimes 1_A) \circ \eta_Z, \quad \text{i.e.} \quad \text{red } \text{circle with green dot} = \text{green } \text{circle with red dot}. \quad (77)$$

In the updated notation for classical points of COS, the comonoid homomorphism laws governing classical points become



and the mutual unbiasedness conditions become

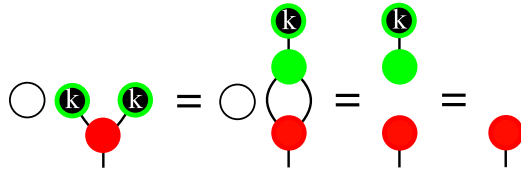


**Theorem 8.3** (complementarity  $\Rightarrow$ ). *Let  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  be two observable structures whose induced  $\dagger$ -compact structures coincide. If they obey*

$$D \cdot \delta_X \circ \delta_Z^\dagger = \epsilon_X^\dagger \circ \epsilon_Z, \quad \text{i.e.} \quad \text{Diagram (78)}$$

then they are complementary observable structures. We call (78) the ‘Hopf law’.

**Proof.** We have to show that **comp1** and **comp2** of definition 8.1 hold. Since:

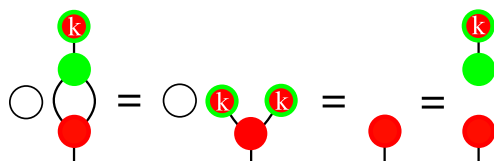


**comp1** holds; by exchanging the colours we obtain **comp2**. □

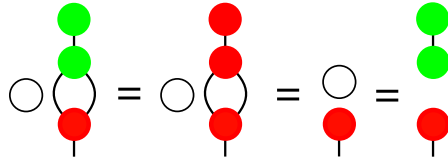
The converse to theorem 8.3 also holds if one of the observable structures involved is either a vector or state basis— cf definition 6.27.

**Theorem 8.4** (complementarity  $\Leftarrow$ ). *If  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  are complementary observable structures, and if at least one of these is either a vector basis or a state basis, then the Hopf law of theorem 8.3 holds.*

**Proof.** We need to show when applying the left-hand side and the right-hand side of the Hopf law to an element of the basis that both sides are equal, for all the elements of the basis. For the case of a vector basis, we have



and for the case of a state basis we moreover have:



where the first equation relies on coinciding  $\dagger$ -compact structures.  $\square$

### 8.2. The general case: dualizers as antipodes

The results of this section still hold when the  $\dagger$ -compact structures induced by the two COS do coincide, provided we extend the observable structures formalism with dualizers, as described in [26] by Paquette, Perdrix and one of the present authors.

**Definition 8.5.** *The dualizer of two distinct observable structures  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  on the same object  $A$  is*

$$d_{ZX} = (\eta_Z \otimes 1_A) \circ (1_A \otimes \eta_X^\dagger), \quad \text{i.e.} \quad \begin{array}{c} \text{red square} \\ | \\ \text{red dot} \end{array} = \begin{array}{c} \text{green dot} \\ \text{red dot} \end{array} . \quad (79)$$

**Remark 8.6.** *If the induced  $\dagger$ -compact structures of the two observable structures on  $A$  happen to coincide, then their dualizer is  $1_A$ , hence trivial. More generally, the dualizer is easily seen to always be unitary, by  $\dagger$ -compactness.*

**Lemma 8.7.** *For observable structures  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$ , we have*

$$(d_{ZX} \otimes 1_A) \circ \eta_X = \eta_Z^\dagger, \quad \text{i.e.} \quad \begin{array}{c} \text{red dot} \\ \text{red square} \end{array} = \begin{array}{c} \text{green dot} \end{array}, \quad (80)$$

and the equation obtained by exchanging the colours also holds.

**Proof.** Straightforward by  $\dagger$ -compactness.  $\square$

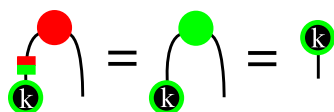
**Remark 8.8.** *Lemma 8.7 together with unitarity of the dualizer provides a more concise proof of the fact that dimension does not depend on the choice of observable structure—cf lemma 6.21.*

**Lemma 8.9.** *Let  $k : \mathbb{1} \rightarrow A$  be a classical point for observable structure  $(A, \delta_Z, \epsilon_Z)$  and let  $(A, \delta_X, \epsilon_X)$  be another observable structure. Then the point*



is the conjugate to  $k$  for the  $\dagger$ -compact structure induced by  $(A, \delta_X, \epsilon_X)$ .

**Proof.** The  $(A, \eta_X)$ -conjugate to  $d_{ZX} \circ k$  is, using lemma 8.7,



since the  $(A, \eta_Z)$ -transpose to  $k$  is also its adjoint.  $\square$

**Theorem 8.10.** *If two observable structures obey*

$$D \cdot \delta_X \circ (d_{ZX} \otimes 1_A) \circ \delta_Z^\dagger = \epsilon_X^\dagger \circ \epsilon_Z, \quad \text{i.e.} \quad \text{Diagram 1} = \text{Diagram 2}, \quad (81)$$

*then they are complementary observable structures. Conversely, if  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  are complementary observable structures, and if at least one of these is either a vector basis or a state basis, then the Hopf law depicted above holds.*

**Proof.** Using lemmas 8.7 and 8.9, the proofs of theorems 8.3 and 8.4 can be easily modified to this more general situation.  $\square$

**Remark 8.11.** *In the form (81), the Hopf law matches the form of the defining law of a Hopf algebra [13, 50, 73], with the dualizer playing the role of the antipode.*

### 9. Closed complementary observable structures

In this section, we study a special class of complementary observable structures, which we refer to as *closed*. While in the previous section we recovered the **B'**-rule of the ZX-calculus, which captures complementarity on-the-nose, the **B**-rules capture this stronger form of complementarity for observable structures. The main theorem of this section provides a number of equivalent characterizations of closedness. The bottom line will be that certain pairs of observable structures form a scaled variant of the usual notion of a *bialgebra* [13, 50, 73]. The defining equations of a bialgebra involve a commutation condition of the multiplication of one algebra with the comultiplication of the other, as well as one of the (co)multiplication of one algebra with the (co)unit of the other. We identify the scaled analogues to these conditions for closed complementary observable structures in sections 9.2 and 9.1, respectively. Again, we assume that the  $\dagger$ -compact structures induced by the complementary observable structures coincide.

#### 9.1. Coherence for observable structures

In this section, we provide a category-theoretic generalization of the concrete notion of coherence for complementary vector and state bases—cf definition 5.7. The green and red observable structures of the ZX-calculus also enjoy this property. First we set

$$\blacklozenge = \text{Diagram}$$

and denote this scalar by  $\sqrt{D}$  for reasons we explain below.

**Definition 9.1.** *Two observable structures  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  in a  $\dagger$ -SMC are called coherent if they obey the following two rules:*

**coher1** $\epsilon_X$  *satisfies*

$$\sqrt{D} \cdot \delta_Z \circ \epsilon_X^\dagger = \epsilon_X^\dagger \otimes \epsilon_X^\dagger, \quad \text{i.e.} \quad \text{Diagram 1} = \text{Diagram 2},$$

**coher2** $\epsilon_Z$  satisfies

$$\sqrt{D} \cdot \delta_X \circ \epsilon_Z^\dagger = \epsilon_Z^\dagger \otimes \epsilon_X^\dagger, \quad \text{i.e.} \quad \begin{array}{c} \color{green}\bullet \\ \color{red}\blacklozenge \end{array} = \begin{array}{cc} \color{green}\bullet & \color{green}\bullet \\ | & | \end{array}.$$

**Remark 9.2.** As already mentioned in the introduction of this section, the conditions **coher1** and **coher2** are scaled variants of two of the defining conditions of a bialgebra; in the language of this paper, these state that the erasing point of one observable structure is a classical point for the other. Condition **coher1** in definition 9.1 states that  $\epsilon_X^\dagger$  differs from a classical point of  $(A, \delta_Z, \epsilon_Z)$  by a scalar factor of  $\sqrt{D}$ . The choice of  $\sqrt{D} = (\epsilon_Z^\dagger \circ \epsilon_X^\dagger)$  for this scalar is not arbitrary but is imposed by the fact that  $\epsilon_Z$  is the unit for the comultiplication  $\delta_Z$ . To see this, it suffices to post-compose both sides of **coher1** with  $\epsilon_Z \otimes \epsilon_X$ , which results in

$$\begin{array}{c} \color{red}\bullet \\ | \\ \color{red}\bullet \end{array} \color{red}\blacklozenge = \begin{array}{c} \color{red}\bullet \\ | \\ \color{red}\bullet \end{array} \begin{array}{c} \color{green}\bullet \\ | \\ \color{green}\bullet \end{array} = \begin{array}{cc} \color{red}\bullet & \color{red}\bullet \\ | & | \\ \color{red}\bullet & \color{green}\bullet \end{array} = \begin{array}{c} \color{red}\bullet \\ | \\ \color{red}\bullet \end{array} \begin{array}{c} \color{green}\bullet \\ | \\ \color{green}\bullet \end{array} \color{red}\blacklozenge.$$

Dually, condition **coher2** asserts the same relationship between  $\epsilon_Z^\dagger$  and  $(A, \delta_X, \epsilon_X)$ .

**Example 9.3.** For the case of **FdHilb** and **FdHilb<sub>wp</sub>** this category-theoretic notion of coherence coincides with that of definition 5.7. For these cases, theorem 5.9 indicates that the requirement of coherence entails no loss of generality.

Now we justify the notation  $\sqrt{D}$  for  $\color{red}\blacklozenge$ .

**Lemma 9.4.** If  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  are two observable structures whose induced  $\dagger$ -compact structures coincide, then we have:

$$\sqrt{D}^\dagger = \sqrt{D}, \quad \text{i.e.} \quad \color{green}\blacklozenge = \color{red}\blacklozenge.$$

**Proof.** By corollary 6.18, we know that  $\epsilon_Z$  and  $\epsilon_X$  are both self-conjugate; hence:

$$\begin{array}{c} \color{red}\bullet \\ | \\ \color{green}\bullet \end{array} = \begin{array}{c} \color{red}\bullet \\ \color{red}\bullet \end{array} \begin{array}{c} \color{green}\bullet \\ \color{green}\bullet \end{array} = \begin{array}{c} \color{green}\bullet \\ | \\ \color{red}\bullet \end{array}. \tag{82}$$

The result follows from the fact that the dualizer is trivial when the induced  $\dagger$ -compact structures coincide. □

By using the notation  $\sqrt{D}$  for  $\color{red}\blacklozenge$ , we insinuate that

$$\color{red}\blacklozenge \color{green}\blacklozenge = \sqrt{D} \cdot \sqrt{D} = D = \bigcirc, \tag{83}$$

which by, lemma 9.4, becomes

$$\begin{array}{cc} \color{green}\bullet & \color{red}\bullet \\ \color{red}\bullet & \color{green}\bullet \end{array} = \color{red}\blacklozenge \color{green}\blacklozenge = \bigcirc. \tag{84}$$

Since the ‘length’ of both  $\epsilon_Z^\dagger$  and  $\epsilon_X^\dagger$  is  $\sqrt{D}$ —cf lemma 7.16—i.e.

$$\begin{array}{c} \bullet \\ \bullet \end{array} = \bigcirc, \quad \begin{array}{c} \bullet \\ \bullet \end{array} = \bigcirc, \quad (85)$$

equation (84) states that  $\epsilon_Z^\dagger$  and  $\epsilon_X^\dagger$  are unbiased, which is a natural requirement for a pair of COS. Moreover, it follows from coherence of observable structures that:

**Proposition 9.5.** *For coherent observable structures on  $A$  with coinciding induced  $\dagger$ -compact structures, we have*

$$\sqrt{D} \cdot \sqrt{D} = D = \dim(A), \quad \text{i.e.} \quad \blacklozenge \blacklozenge = \bigcirc. \quad (86)$$

**Proof.** We have

$$\blacklozenge \blacklozenge = \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} = \bigcirc$$

where the last step uses coincidence of induced  $\dagger$ -compact structures. □

### 9.2. Commutation for observable structures

Several notions of commutation may apply to observable structures. In this section, we consider three of these, one of which will complete the definition of a scaled bialgebra; in the ZX-calculus, this is the powerful **B2**-rule.

**Remark 9.6.** *One should clearly distinguish the notions of commutation that we consider in this paper from that of commuting observables as found in most of the quantum theory literature. The kind of observables considered here are complementary, and are thus non-commuting in the usual sense. What we wish to expose here is that certain alternative notions of commutation, which are useful in computations, do apply for the specific case of complementary observables.*

*Notation.* For an observable structure  $(A, \delta_Z, \epsilon_Z)$ , with classical points  $\mathcal{K}_Z$  depicted in green, and an observable structure  $(A, \delta_X, \epsilon_X)$  depicted in red, we set for all  $k \in \mathcal{K}_Z$ :

$$\begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)} := \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)}.$$

The use of two colours in this graphical representation reflects its dependence on two observable structures. We denote this morphism by  $\Lambda^X(k)$ . By lemma 7.15 we know that, when  $k$  is unbiased for  $(A, \delta_X, \epsilon_X)$ , this morphism is unitary if and only if  $k^\dagger \circ k = D$ . Therefore, it is more convenient to consider classical points to have length  $\sqrt{D}$  rather than being normalized. The comonoid homomorphism laws governing classical points then become

$$\begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)} = \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)} \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)}, \quad \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)} = \blacklozenge, \quad \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)} = \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)} \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)}, \quad \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)} = \blacklozenge$$

where we somewhat abusively depict  $\sqrt{D}$  by  $\blacklozenge$  as in the case of coherent observable structures. If these observables are complementary, the equations of definition 8.1 become

$$\begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)} \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)} = \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)}, \quad \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (red)} \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)} = \begin{array}{c} \bullet \\ \bullet \end{array} \text{ (green)}.$$



**Remark 9.7.** The similarity between the graphical notation for  $\Lambda^X(k)$  and that of the classical points for COS in section 8 anticipates theorem 9.24 below.

**Definition 9.8.** Observable structure  $(A, \delta_Z, \epsilon_Z)$  with classical points  $\mathcal{K}_Z$ , and observable structure  $(A, \delta_X, \epsilon_X)$  with classical points  $\mathcal{K}_X$ , obey operator commutation iff for all  $k \in \mathcal{K}_Z$  and all  $k' \in \mathcal{K}_X$

$$\Lambda^Z(k') \circ \Lambda^X(k) = (k'^{\dagger} \circ k) \cdot (\Lambda^X(k) \circ \Lambda^Z(k')), \quad \text{i.e.} \quad \begin{array}{c} \color{red}\blacklozenge \\ \color{green}\textcircled{k} \\ \color{red}\textcircled{k} \end{array} = \begin{array}{cc} \color{green}\textcircled{k} & \color{green}\textcircled{k} \\ \color{red}\textcircled{k} & \color{red}\textcircled{k} \end{array}.$$

**Definition 9.9.** Observable structure  $(A, \delta_Z, \epsilon_Z)$  with classical points  $\mathcal{K}_Z$ , and observable structure  $(A, \delta_X, \epsilon_X)$ , obey comultiplicative commutation iff for all  $k \in \mathcal{K}_Z$

$$\delta_Z \circ \Lambda^X(k) = (\Lambda^X(k) \otimes \Lambda^X(k)) \circ \delta_Z, \quad \text{i.e.} \quad \begin{array}{c} \color{green}\textcircled{k} \\ \color{green}\textcircled{k} \end{array} = \begin{array}{cc} \color{green}\textcircled{k} & \color{green}\textcircled{k} \\ \color{red}\textcircled{k} & \color{red}\textcircled{k} \end{array}.$$

**Remark 9.10.** While this equation seems akin to the defining equation for classical points, it carries a lot more structure. The reason for this is the involvement of two observable structures, which is exposed by the colouring.

**Definition 9.11.** Observable structures  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  obey bialgebraic commutation iff

$$D \cdot (\delta_X^{\dagger} \otimes \delta_X^{\dagger}) \circ (1 \otimes \sigma \otimes 1) \circ (\delta_Z \otimes \delta_Z) = \sqrt{D} \cdot \delta_Z \circ \delta_X^{\dagger}, \quad \text{i.e.} \quad \begin{array}{c} \color{green}\textcircled{k} & \color{green}\textcircled{k} \\ \color{red}\textcircled{k} & \color{red}\textcircled{k} \end{array} = \begin{array}{c} \color{red}\blacklozenge \\ \color{green}\textcircled{k} \end{array}.$$

**Remark 9.12.** For coherent observable structures, by proposition 9.5, when  $\sqrt{D}$  admits an inverse we can simplify the bialgebraic commutation equation to

$$\begin{array}{c} \color{red}\blacklozenge \\ \color{green}\textcircled{k} & \color{green}\textcircled{k} \\ \color{red}\textcircled{k} & \color{red}\textcircled{k} \end{array} = \begin{array}{c} \color{red}\textcircled{k} \\ \color{green}\textcircled{k} \end{array}.$$

To see that the choice of scalars is not arbitrary, we can, for example, either assume coherence or the Hopf law for the observable structures, both resulting in

$$\begin{array}{c} \color{red}\textcircled{k} \\ \color{green}\textcircled{k} \\ \color{red}\textcircled{k} \\ \color{green}\textcircled{k} \end{array} = \begin{array}{c} \color{red}\textcircled{k} \\ \color{green}\textcircled{k} \\ \color{red}\textcircled{k} \\ \color{green}\textcircled{k} \end{array} = \begin{array}{c} \color{green}\textcircled{k} & \color{red}\textcircled{k} \\ \color{green}\textcircled{k} & \color{red}\textcircled{k} \\ \color{green}\textcircled{k} & \color{red}\textcircled{k} \\ \color{green}\textcircled{k} & \color{red}\textcircled{k} \end{array} = \begin{array}{c} \color{green}\textcircled{k} & \color{red}\textcircled{k} \\ \color{red}\textcircled{k} & \color{green}\textcircled{k} \\ \color{green}\textcircled{k} & \color{red}\textcircled{k} \\ \color{red}\textcircled{k} & \color{green}\textcircled{k} \end{array} = \begin{array}{c} \color{red}\textcircled{k} \\ \color{green}\textcircled{k} \end{array}.$$

**Definition 9.13.** A scaled bialgebra is a pair of coherent observable structures that satisfy bialgebraic commutation, that is, all together:

$$\begin{array}{c} \color{red}\blacklozenge \\ \color{green}\textcircled{k} \end{array} = \begin{array}{cc} \color{green}\textcircled{k} & \color{green}\textcircled{k} \\ \color{red}\textcircled{k} & \color{red}\textcircled{k} \end{array} \quad \begin{array}{c} \color{green}\textcircled{k} & \color{green}\textcircled{k} \\ \color{red}\textcircled{k} & \color{red}\textcircled{k} \end{array} = \begin{array}{c} \color{red}\blacklozenge \\ \color{green}\textcircled{k} \end{array}.$$

**Remark 9.14.** As announced above, if we remove the scalars from the definition of a scaled bialgebra and adjoin the equation  $\epsilon_Z \circ \epsilon_X^\dagger = 1_I$ —which is trivial anyway when taken ‘up to a scalar’—then we obtain the usual notion of a bialgebra [13, 50, 73].

**Theorem 9.15.** Each scaled bialgebra satisfies the Hopf law.

**Proof.** See the derivation of the **B'**-rule in section 2.2; note that the 1st step uses  $\dagger$ -compactness and the 4th step uses coherence i.e. the green comultiplication copies the red unit.  $\square$

**Corollary 9.16.** If a pair of observable structures constitutes a scaled bialgebra, then these are complementary observable structures.

While at first sight the three notions of commutation we have introduced in this section look very different, in fact, they boil down to the same thing in all of our example categories, as we shall see in theorem 9.24 below.

### 9.3. Closedness for observable structures

**Definition 9.17.** The classical points  $\mathcal{K}_Z$  of an observable structure  $(A, \delta_Z, \epsilon_Z)$  are closed for another observable structure  $(A, \delta_X, \epsilon_X)$  iff for all  $k, k' \in \mathcal{K}_Z$  we have

$$k \odot_X k' \in \mathcal{K}_Z.$$

From the assumption that the induced  $\dagger$ -compact structures coincide, since by corollary 6.18 and definition 6.23 we have that  $\delta_X, k$  and  $k'$  are all self-conjugate, it follows that the composite  $k \odot_X k'$  is also self-conjugate. Hence, setting:

the closedness requirement is depicted graphically as

**Remark 9.18.** If the observable structures are coherent, then the normalization condition is also trivially satisfied. If classical points were taken to be normalized, then we would take  $\sqrt{D} \cdot k \odot_X k'$  rather than  $k \odot_X k'$  in definition 9.17.

**Remark 9.19.** Again, similarly to remark 9.7, this notation that seems to indicate that  $k \odot_X k'$  is unbiased to  $(A, \delta_X, \epsilon_X)$  anticipates theorem 9.24 below.

We now show that on every Hilbert space we can find a pair of closed COS, and hence by theorem 5.9 we can find a pair of closed coherent COS.

**Proposition 9.20.** In *FdHilb* there exist pairs of closed coherent COS on Hilbert spaces  $\mathbb{C}^n$  for any dimension  $n \in \mathbb{N}$ .

**Proof.** Without loss of generality we take the first observable structure as being defined by the standard basis on  $\mathbb{C}^n$ , i.e.  $\delta : |i\rangle \mapsto |i\rangle \otimes |i\rangle$  with the erasing point  $\epsilon^\dagger = \sum_i |i\rangle$ . Note that the multiplication induced by this observable structure is point-wise:

$$\left( \sum_i a_i |i\rangle \right) \odot \left( \sum_i b_i |i\rangle \right) = \sum_i a_i b_i |i\rangle.$$

We need to find a basis which contains  $\epsilon^\dagger$ , is unbiased with respect to the standard basis and is closed under  $\odot$ . It is routine to check that the family

$$|f_j\rangle = \frac{1}{\sqrt{N}} \sum_k \omega_n^{jk} |k\rangle,$$

where  $j$  and  $k$  range from 0 to  $n - 1$ , and  $\omega_n = e^{2\pi i/n}$ , provides an orthonormal basis satisfying these conditions. We choose  $|0\rangle$  as the erasing point.  $\square$

**Corollary 9.21.** *There exist pairs of closed coherent complementary observable structures for any dimension in  $\mathbf{FdHilb}_{wp}$ .*

**Remark 9.22.** *Thanks to theorem 5.9, to find a pair of coherent COS on  $\mathbb{C}^d$  it suffices to find any dephased complex Hadamard matrix, that is, an orthogonal matrix whose entries are all complex units, and whose first row and column are all ones. The columns of the matrix will provide the required basis. The family  $|f_j\rangle$  used above are a particular example: they form the columns of the  $d$ -dimensional Fourier matrix. If  $d = 2, 3$  or  $5$  the only dephased Hadamards are Fourier matrices [74]; hence we can conclude that every pair of coherent COS in these dimensions is closed. However, this does not hold in general. If  $d = 4$ , for example,*

$$F_4(x) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & ie^{ix} & -1 & -ie^{ix} \\ 1 & -1 & 1 & -1 \\ 1 & -ie^{ix} & -1 & ie^{ix} \end{pmatrix}$$

*is not closed when  $x$  is irrational. Similar counterexamples can be constructed for dimensions  $d \geq 6$ . This shows that the notion of closed COS is strictly stronger than that of COS.*

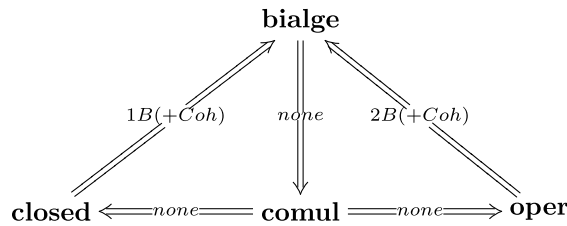
Since closed COS exist for all dimensions, for most practical purposes we can assume that COS are both coherent and closed. Closed COS moreover behave well with respect to the monoidal structure, in that the canonical induced observable structures of proposition 6.28, which are defined on the tensor space, inherit both complementarity and closedness.

**Proposition 9.23.** *Let  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  be coherent COS such that  $(\delta_Z, \epsilon_Z)$  is closed with respect to  $(\delta_X, \epsilon_X)$ , and let  $(B, \delta_{Z'}, \epsilon_{Z'})$  and  $(B, \delta_{X'}, \epsilon_{X'})$  be coherent COS such that  $(\delta_{Z'}, \epsilon_{Z'})$  is closed with respect to  $(\delta_{X'}, \epsilon_{X'})$ ; then the canonical observable structure on the joint space  $(A \otimes B, \delta_Z \otimes \delta_{Z'}, \epsilon_Z \otimes \epsilon_{Z'})$  is both complementary and closed with respect to  $(A \otimes B, \delta_X \otimes \delta_{X'}, \epsilon_X \otimes \epsilon_{X'})$ .*

9.4. Our main theorem on pairs of closed observable structures

**Theorem 9.24.** *The following are equivalent for two observable structures:*

- closed** *They are closed.*
  - oper** *They obey operator commutation.*
  - comul** *They obey comultiplicative commutation.*
  - bialge** *They obey bialgebraic commutation.*
- subject to the following requirements:*



where ‘none’ stands for no additional requirements, except for the ones explicitly stated in the proof; where ‘1B’ means that at least one of the observable structures has either a vector basis or a state basis, where ‘2B’ means that this is the case for both observable structures, and ‘(+ Coh)’ means that in the case of state bases we also require coherence. We indicate in the proof where we assume that  $\sqrt{D}$  has an inverse and where we use the fact that  $\dagger$ -compact structures coincide.

**Proof.** We show all required implications graphically:

- **bialge  $\Rightarrow$  comul:**

Here we assumed that  $\sqrt{D}$  has an inverse.

- **comul  $\Rightarrow$  closed:**

- **comul  $\Rightarrow$  oper:**

- **closed  $\Rightarrow$  bialge:**

The assumption that the classical points for the green observable structure constitute a vector basis, together with the fact that the monoidal tensor lifts vector bases, implies bialgebraic commutation. By coherence we have

$$(91)$$

so the result holds when there is a state basis for the green observable structure. Steps 2–4 assume that the induced  $\dagger$ -compact structures coincide.

- **oper  $\Rightarrow$  bialge:**

$$(92)$$

so by  $\dagger$ -compactness we have:

$$(93)$$

Under the assumption that the classical points both for the green and the red observable structure constitute a vector basis, together with the fact that the monoidal tensor lifts vector bases, we have

$$(94)$$

from which the bialgebra follows by  $\dagger$ -compactness. The two diamonds are equal to a circle given that the  $\dagger$ -compact structures coincide. For the case where both observable structures have a state basis, it remains to be shown that

$$(95)$$

To do so, we now show that the equation

$$(96)$$

holds, by relying on the fact that we have a state basis for both observable structures, and as above, by again relying on  $\dagger$ -compactness. We have

$$(97)$$

where in the dotted area we used derivation (92) above. Finally,

$$(98)$$

where the last step assumes that induced  $\dagger$ -compact structures coincide.

This concludes this proof.  $\square$

**Remark 9.25.** We leave it to the reader to see how ‘2B (+ Coh)’ factors into requirements for *oper*  $\Rightarrow$  *comul* and *comul*  $\Rightarrow$  *bialge*.

The examples of COS discussed in proposition 9.20 satisfy all the equations stated in theorem 9.24. In particular, they constitute scaled bialgebras. These equations are strictly stronger than the Hopf law by theorem 9.15, and hence all pairs of observable structures that satisfy them are COS.

## 10. Further group structure and the classical automorphisms

In section 7.4, we saw how the Abelian group of phase shifts arose naturally from the presence of unbiased points for a given observable structure. When we have a pair of COS, the two phase groups can interfere with each other, an interaction that arises from the special role of the classical points within each phase group.

In the following, suppose that  $(A, \delta_Z, \epsilon_Z)$  and  $(A, \delta_X, \epsilon_X)$  are coherent COS which jointly form a scaled bialgebra. Let  $\mathcal{U}_Z$  denote all the unbiased points for  $(\delta_Z, \epsilon_Z)$ , and let  $\mathcal{K}_Z$  denote its classical points; define  $\mathcal{U}_X$  and  $\mathcal{K}_X$  similarly. By virtue of complementarity we have  $\mathcal{K}_X \subseteq \mathcal{U}_Z$  and  $\mathcal{K}_Z \subseteq \mathcal{U}_X$ . Recall that by proposition 7.19,  $(\mathcal{U}_Z, \odot_Z)$  is an Abelian group, isomorphic to the phase group of  $(\delta_Z, \epsilon_Z)$ .

**Theorem 10.1.**  $\mathcal{K}_X$  is a subgroup of  $(\mathcal{U}_Z, \odot_Z)$  either if  $\mathcal{K}_X$  is finite or if the two observable structures give rise to the same  $\dagger$ -compact structure.

**Proof.**  $\mathcal{K}_X$  is always a submonoid of  $\mathcal{U}_Z$  because of the closure and coherence of the two observable structures; any finite submonoid is a subgroup. Alternatively, given a point  $x \in \mathcal{K}_X$ , its inverse in  $\mathcal{U}_Z$  is given by its conjugate with respect to the  $\dagger$ -compact structure of  $(\delta_Z, \epsilon_Z)$ ; by the definition of classicality,  $x$  is self-conjugate with respect to the  $\dagger$ -compact structure of  $(\delta_X, \epsilon_X)$ . Hence, if these  $\dagger$ -compact structures agree (cf proposition 8.2),  $x^{-1} = x$  in  $\mathcal{U}_Z$ , so  $\mathcal{K}_X$  is a subgroup.  $\square$

**Remark 10.2.** Shared  $\dagger$ -compact structure is a powerful assumption. The proof above indicates that in the case of coinciding  $\dagger$ -compact structures, not only do the classical points within  $\mathcal{U}_Z$  form a subgroup, but the resulting group is a product of copies of  $S_2$ . In the case of qubits described by  $X$  and  $Z$  spins, the  $\dagger$ -compact structure is shared, and the resulting classical subgroup is just  $S_2$ .

**Proposition 10.3.** For all  $x \in \mathcal{K}_X$ ,  $\Lambda^Z(x)$  is a left action on  $\mathcal{U}_Z$  and, in particular, is a permutation on  $\mathcal{K}_X$ .

**Proof.** For any  $\psi : I \rightarrow A$ , we have  $\Lambda^Z(x) \circ \psi = x \odot_Z \psi$  by definition; that this is a permutation on  $\mathcal{K}_X$  follows from the closure of  $\mathcal{K}_X$ .  $\square$

**Theorem 10.4.** Suppose that  $k \in \mathcal{K}_Z$ , and define  $K = \Lambda^X(k)$ ; then  $K$  is a group automorphism of  $\mathcal{U}_Z$ .

**Proof.** Graphically we depict  $K$  as:

$$K = \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} . \tag{99}$$

Since  $k \in \mathcal{U}_X$ ,  $K$  is unitary and hence is invertible. We must show that if  $\alpha \in \mathcal{U}_Z$  then also  $K \circ \alpha \in \mathcal{U}_Z$ . This holds if and only if  $\Lambda^Z(K \circ \alpha)$  is unitary; we show this directly:

$$\begin{array}{c} \Lambda^Z(K(\alpha)) \\ \hline \Lambda^Z(K(\alpha))^\dagger \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \begin{array}{c} | \\ \bullet \\ | \end{array} \tag{100}$$

where the equations are by the comultiplication property, the unitarity of  $K$ , the unbiasedness of  $\alpha$  and the unitarity of  $K$  again. It remains to be shown that  $K$  is a homomorphism of the group structure.

(i)  $K \circ (\alpha \odot_Z \beta) = (K \circ \alpha) \odot_Z (K \circ \beta)$ :

$$\begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} . \tag{101}$$

The equations are: the definition of  $K$ ; the bialgebra law; the classical property of  $k$ ; and the definition of  $K$ .

(ii)  $K \circ \epsilon_Z^\dagger = \epsilon_Z^\dagger$  (up to global phase):

$$\begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} = \begin{array}{c} \bullet \\ | \end{array} \begin{array}{c} \bullet \\ | \end{array} . \tag{102}$$

The equation simply uses coherence of  $\delta_X$  and  $\epsilon_Z$ ; the result follows by dividing by the scalar factor as per lemma 7.16.

(iii)  $(K \circ \alpha)^{-1} = K \circ \alpha^{-1}$ :

$$\text{Diagrammatic equation (103)} \tag{103}$$

where we relied upon the comultiplication property of  $K$  and the unbiasedness of  $\alpha$ , showing that the inverse  $K \circ \alpha$  in  $\mathcal{U}_Z$  is  $K \circ \alpha^{-1}$  as required.

Hence,  $K$  is an automorphism of  $\mathcal{U}_Z$ . □

**Corollary 10.5.**  $(\mathcal{K}_Z, \odot_X)$  is an Abelian group of automorphisms on  $\mathcal{U}_Z$  whose action is defined by  $(x, z) \mapsto \Lambda^X(x) \circ z$ .

The possibility that the classical points will act as automorphisms on the corresponding phase group gives rise to ‘interference’ phenomena; this is illustrated by the example of the quantum Fourier transform of section 3.2.3.

In the following section we provide an example of the structure exposed in this section, for the spin  $Z$  and  $X$  observables, and show its role in the  $ZX$ -calculus.

### 11. Deriving the ZX-calculus

The preceding sections derived the basic properties of complementary observable structures in an arbitrary  $\dagger$ -SMC. The resulting theory, although very rich, may feel rather abstract. This abstraction is a necessary consequence of working with arbitrary observable structures, without specifying exactly what they are. In any concrete setting, given a fixed pair of observable structures, the remainder of the structure can be constructed via simple direct computations.

This section will focus on a single concrete example and demonstrate how to construct all the structures found in the earlier part of the paper for a given pair of complementary observables. Working in the category of finite dimensional Hilbert spaces, we choose a pair of complementary observable structures over  $\mathbb{C}^2$ —those corresponding to the  $Z$  and  $X$  spin observables—and show how this choice produces a concrete graphical theory for reasoning about qubits. The resulting theory is the  $ZX$ -calculus of sections 2 and 3: this section will justify the simplified syntax of the  $ZX$ -calculus and show that the rules of the calculus (shown in Figure 1) can be derived from the theorems of the preceding sections.

As already noted in examples 4.10 and 4.19, the category of finite dimensional Hilbert spaces is a  $\dagger$ -SMC, and hence the use of graphical notation is justified by theorem 4.24. This is already enough to justify the first two generators of the  $ZX$ -calculus, namely the straight and crossing wires. Since qubits are the only system of interest, the type labels will be dropped from the edges of diagrams: all edges are implicitly labelled by  $\mathbb{C}^2$ . Having introduced the edges, we now turn to the vertices.

The first vertices to be considered are those defining the ‘green’ observable structure  $(\delta_Z, \epsilon_Z)$ , corresponding to the  $Z$ -spin observable, which is defined on  $\mathbb{C}^2$  via the linear maps,

$$\delta_Z : |i\rangle \mapsto |ii\rangle \qquad \epsilon_Z : \sqrt{2}|+\rangle \mapsto 1$$



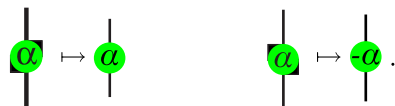
As discussed in example 7.22, the points that are unbiased for  $(\delta_Z, \epsilon_Z)$  have the form  $|\alpha_Z\rangle = |0\rangle + e^{i\alpha}|1\rangle$ , where  $0 \leq \alpha < 2\pi$ , and hence the phase group consists of matrices of the form

$$\Lambda^Z(|\alpha_Z\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} = \begin{array}{c} | \\ \bullet \\ | \end{array}.$$

The group  $(\mathcal{U}_Z, \odot_Z)$  is therefore isomorphic to the circle, and the operation  $\odot_Z$  is addition modulo  $2\pi$ . The Pauli-Z matrix is given by  $\Lambda^Z(\pi)$ . Note also that

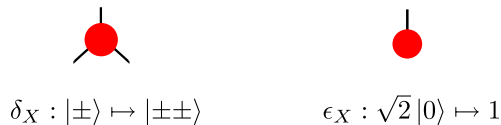
$$\begin{array}{c} | \\ \bullet \\ | \end{array} = \left( \begin{array}{c} | \\ \bullet \\ | \end{array} \right)^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} = \begin{array}{c} | \\ \bullet \\ | \end{array}.$$

so we can drop the ‘corners’ from the diagrammatic notation and simply write the negative angle in its place.



The spider rules (theorem 7.11) justify the first part of the ZX-calculus syntax, the family of ‘green’ vertices  $Z_n^m(\alpha)$ , along with rule (S1) and the first part of rule (S2).

The X-observable structure is essentially the same: defining  $(\delta_X, \epsilon_X)$  as follows:



it is easy to verify that the corresponding phase group consists of rotations around  $X$ , that is, matrices of the form

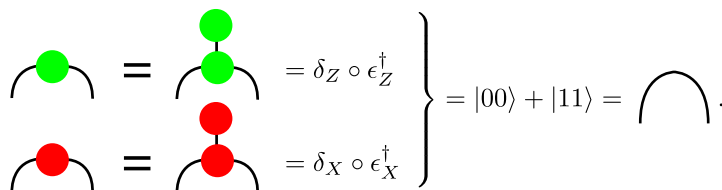
$$\Lambda^X(|\alpha_X\rangle) = \begin{pmatrix} \cos \frac{\alpha}{2} & i \sin \frac{\alpha}{2} \\ i \sin \frac{\alpha}{2} & \cos \frac{\alpha}{2} \end{pmatrix} = \begin{array}{c} | \\ \bullet \\ | \end{array},$$

generated by the (unnormalized) unbiased points  $|\alpha_X\rangle = \sqrt{2}(\cos \frac{\alpha}{2}|0\rangle + i \sin \frac{\alpha}{2}|1\rangle)$ . We can simplify the notation as we did for the  $Z$ -observable:














Of course, the decorated spider rules also apply to  $(\delta_X, \epsilon_X)$ , and this produces the ‘red’ family of the ZX-calculus, the vertices  $X_n^m(\alpha)$ .

To complete rule (S2), we appeal to one property not derived from the formalism of complementary observables, namely the fact that  $(\delta_Z, \epsilon_Z)$  and  $(\delta_X, \epsilon_X)$  induce the same compact structure:



**Table 1.** Translation between general and simplified graphical notation.

General:							
Simplified:					Not allowed		

Hence, we obtain the remaining part of rule (S2), as well as the bending wires.

Further, since each object now comes with a unique  $\dagger$ -compact structure, we can treat the category as  $\dagger$ -compact, and appeal to theorem 4.26. This justifies rule (T), ‘only the topology matters’.

Having noted that  $(\delta_Z, \epsilon_Z)$  and  $(\delta_X, \epsilon_X)$  generate the same  $\dagger$ -compact structure, we may also appeal to lemma 9.4, that is

$$\begin{array}{c} \bullet \\ \bullet \end{array} = \begin{array}{c} \blacklozenge \\ \blacklozenge \end{array} = \begin{array}{c} \blacklozenge \\ \blacklozenge \end{array} = \begin{array}{c} \bullet \\ \bullet \end{array}.$$

Now, setting  $\blacklozenge = \blacklozenge$  (D1), proposition 9.5 produces rule (D2) of the ZX-calculus.

The definition of  $\delta_Z$  immediately shows that the classical points of the  $Z$  observable are  $|0\rangle$  and  $|1\rangle$ ; these points are unbiased for  $(\delta_X, \epsilon_X)$ , corresponding to the angles 0 and  $\pi$  in  $(\mathcal{U}_X, \odot_X)$ . Similarly, the classical points of  $\delta_X$  are  $|+\rangle$  and  $|-\rangle$ , which are unbiased for  $(\delta_Z, \epsilon_Z)$ , and again correspond to the angles 0 and  $\pi$ . This being the case, we can again simplify the graphical notation, and dispense with the two-coloured dots used in sections 8 and 9 in favour of a simpler convention:









*a dot is unbiased for the observable structure of the same colour;*


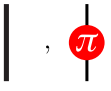
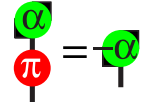

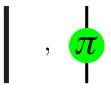
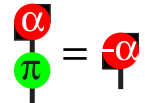
if it is labelled by  $\pi$  or zero then it is classical for the other structure. In the ZX-calculus there is no need for dots of any other kind, so we disallow them. The translation between the more general graphical language and the simplified version used in the ZX-calculus is summarized in table 1.

Since each structure’s classical points are unbiased for the other structure,  $(\delta_Z, \epsilon_Z)$  and  $(\delta_X, \epsilon_X)$  are *complementary* as per definition 8.1. Furthermore, we have  $\epsilon_X^\dagger = \sqrt{2}|0\rangle$  and  $\epsilon_Z^\dagger = \sqrt{2}|+\rangle$ , so the two observable structures are also *coherent* as in definition 9.1, implying rule (B1) of the ZX-calculus.

The classical points of  $Z$  correspond to the angles 0 and  $\pi$  within the phase group of  $X$  and vice versa. Since these angles form a two-element subgroup within the circle group,  $(\delta_X, \epsilon_X)$  and  $(\delta_Z, \epsilon_Z)$  form a *closed* pair of complementary observable structures, as per definition 9.17. Noting that the triple  $\{|0\rangle, |1\rangle, |+\rangle\}$  forms a state basis for  $\mathbb{C}^2$ , the conditions for theorem 9.24 are satisfied: from whence, bialgebraic commutation (definition 9.11) implies rule (B2) and comultiplicative commutation (definition 9.9) implies rule (K1).

**Table 2.** Summary of the group structure for qubits.

Observable	Classical Points	Unbiased Points	Phase Group
$Z = (\delta_Z, \epsilon_Z)$ 	$ 0\rangle,  1\rangle$ 	$ 0\rangle + e^{i\alpha}  1\rangle$ 	$Z_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ 
$X = (\delta_X, \epsilon_X)$ 	$ +\rangle,  -\rangle$ 	$\cos \frac{\alpha}{2}  0\rangle + i \sin \frac{\alpha}{2}  1\rangle$ 	$X_\alpha = \begin{pmatrix} \cos \frac{\alpha}{2} & i \sin \frac{\alpha}{2} \\ i \sin \frac{\alpha}{2} & \cos \frac{\alpha}{2} \end{pmatrix}$ 

Observable	Classical Subgroup	Automorphism Action
$Z = (\delta_Z, \epsilon_Z)$ 	$1, X$ 	$X : Z_\alpha \mapsto Z_{-\alpha}$ 
$X = (\delta_X, \epsilon_X)$ 	$1, Z$ 	$Z : X_\alpha \mapsto X_{-\alpha}$ 

The remaining piece of the structure to be described is the action of  $\mathcal{K}_Z$  on  $\mathcal{U}_Z$  discussed in section 10. Since  $X_1^1(\pi) = X$  we see that the non-trivial element of  $\mathcal{K}_Z$  sends  $|\alpha_Z\rangle \mapsto |-\alpha_Z\rangle$ ;  $X$  assigns elements of  $\mathcal{U}_Z$  to their inverses. The action of  $\mathcal{K}_X$  on  $\mathcal{U}_X$  is exactly dual. This provides the rule (K2) of the ZX-calculus. The group structure is summarized in table 2.

The preceding has shown that the ZX-calculus, with one exception, is readily deduced from the algebraic properties of the  $Z$  and  $X$  observables: indeed everything else followed from that choice. The single exception is the  $H$  vertex and the associated rule (C). The addition of a special symbol for the Hadamard gate is simply to make certain calculations easier, and it is not essential to the calculus.

## 12. Non-determinism, mixed states and classical data flow

The graphical treatment so far has been limited to pure states, and therefore does not capture the full behaviour of quantum measurements, decoherence, classical control, and a host of other phenomena of great practical importance in quantum computation.

This section will present three different extensions of the graphical language to account for mixed states, and dispense with the simplified treatment of measurements as projections. We briefly describe each of these, and provide the same example in each one: the quantum teleportation protocol. For full details, see the references.

The most general is Selinger's CPM construction [68] which, given any category of 'pure states' and 'pure maps', constructs a category of 'mixed states' and 'completely positive maps'. Within the resulting category, Paquette, Pavlovic and one of the present authors defined a plethora of classicality-related concepts such as decoherence, measurement, probability distribution, stochastic map, function on classical data, etc., by relying on observable structure [25]—some of these results were already present in Carboni and Walters' seminal paper [12]. An axiomatic account of Selinger's CPM construction and classical concepts therein was provided by Perdrix and an author of this paper [16, 29]; this introduces a new element into the graphical calculus corresponding to the environment, and a corresponding axiom (and some 'coherence conditions'). Finally, Perdrix and Coecke have introduced a version of the ZX-calculus parameterized by a set of variables that encode the outcome of measurements, and the dependence of other elements on them. These *conditional* diagrams have been used in the context of measurement-based quantum computation to study determinism and information flow [37].

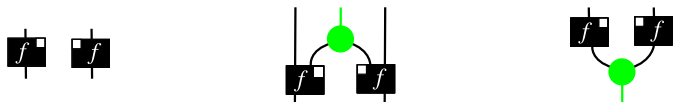
These three approaches are alternatives, and depending on the situation, one may be preferable to another.

### 12.1. The CPM construction and classical concepts therein [25, 68]

We extend the graphical language by a construction that is formally similar to the way in which classical probabilities are described by density operators. Graphically, classical data and classical operations are represented by a single wire, while quantum data and quantum operations are represented by double wires. The passage from a double wire to a single wire via a dot encodes decoherence. This encoding,

$$\frac{1 \text{ wire/box}}{\text{classical}} = \frac{2 \text{ wires/boxes}}{\text{quantum}},$$

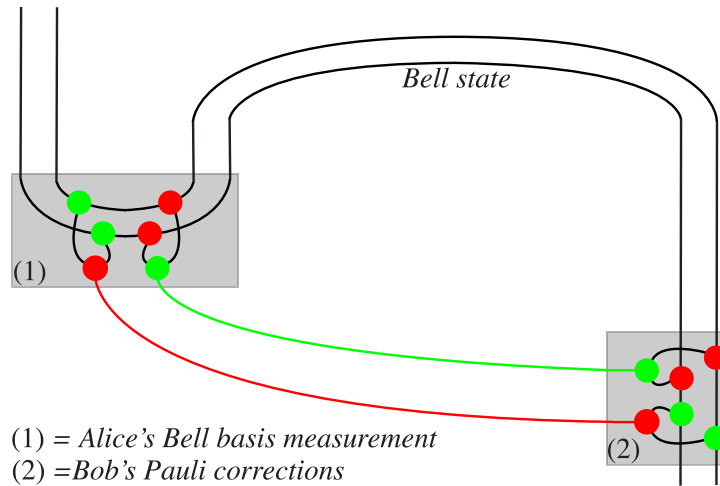
is also present in the Dirac notation; for a mixed state  $\sum_i \omega_i |\psi_i\rangle\langle\psi_i|$  the classical probabilistic state  $(\omega_1, \dots, \omega_n)$  occurs only once, while the quantum states occur both as a ket  $|\psi_i\rangle$  and as a bra  $\langle\psi_i|$ . Pure quantum operations, controlled pure quantum operations and destructive measurements are of the form:



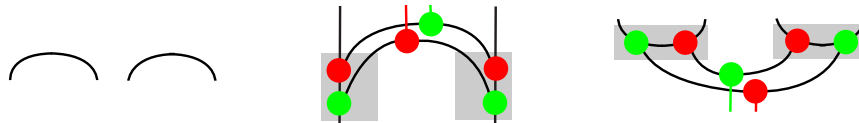
respectively, where for clarity we choose to colour the classical wires in the colour of the observable structure whose classical points will encode the classical data.

In fact, the spiders of the graphical language were initially introduced under the name *classical structures* in [27] to model classical data in quantum informatic protocols. Hence, in this setting, a single concept can account for quantum observables, complementarity and phases, as well as for classical information flow. We will be very brief on the use of spiders in order to describe classical data flow; see [25] for more details.

**Example 12.1.** We claim that the following constitutes the quantum teleportation protocol, including the classical correction:

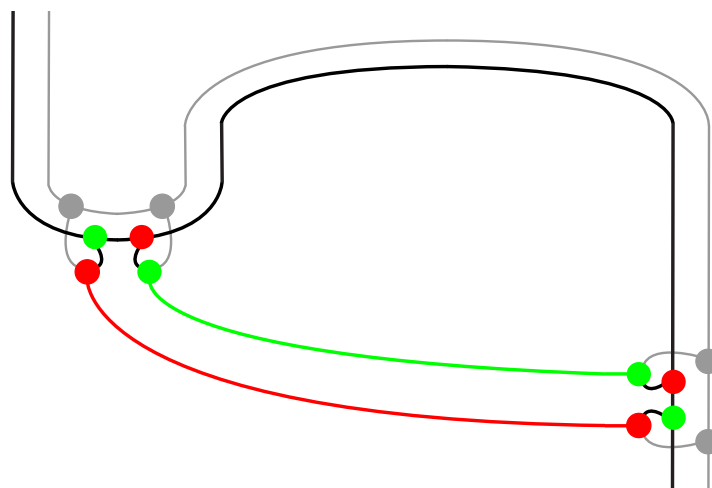


The green and the red wires represent the two qubits Alice has to send to Bob to inform him of the measurement outcome. The Bell state, Bob's Pauli corrections and Alice's Bell basis measurement can be rewritten, respectively, as



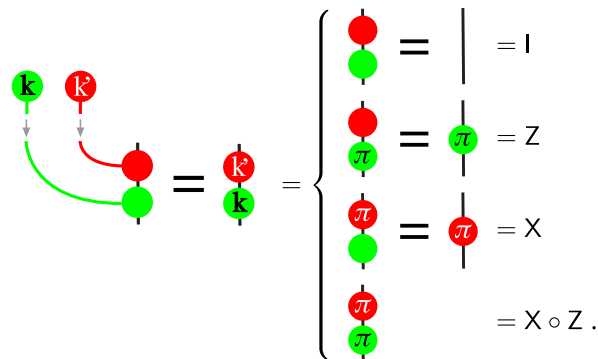
Hence, they are of the forms shown above.

The picture might seem somewhat complicated; the reason for this is that in order to display the quantum-classical distinction graphically, all the quantum operations are doubled. If we hide one of the copies it becomes much clearer what is going on:

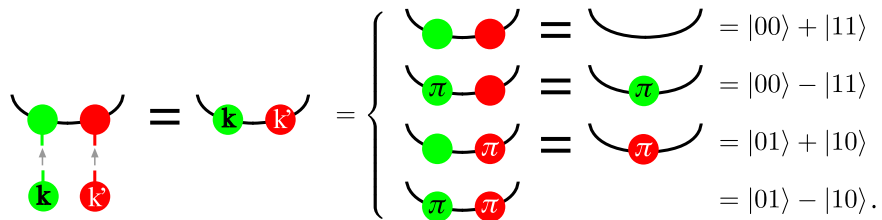


We demonstrate that the measurement and corrections in this picture are indeed the ones we claim them to be. By 'selecting' the control operation, that is, by inserting a classical point

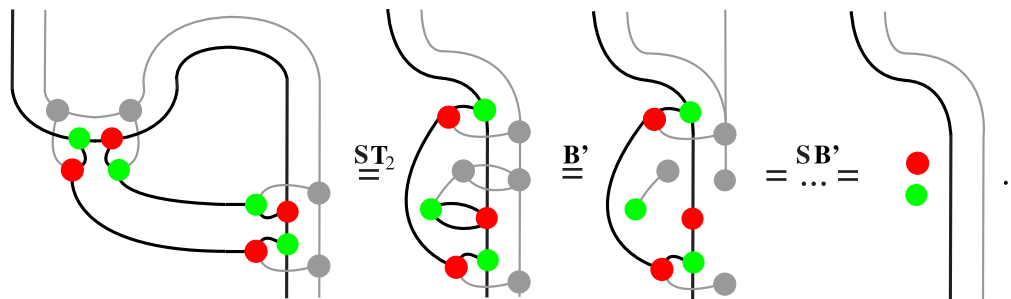
at the input, we obtain the Pauli corrections:



Similarly, by post-‘selecting’ the measurement outcome, that is, by inserting the adjoint of a classical point at the output, we obtain the Bell-basis measurement:



We now compute the overall result of the teleportation protocol diagrammatically:



Note how the **B'**-rule causes the flow of classical data to disconnect from the flow of quantum data, which of course should not depend on classical data anymore. The scalars that remain at the end are a consequence of the fact that we did not normalize the Bell state or the Bell basis measurement or the **B'**-rule; if we had done so, all scalars would have cancelled out.

### 12.2. Classicality via environment [16, 29]

Roughly equivalent to the above ‘construction’ is the following ‘axiomatic account’—see [16] for the precise correspondence. We consider two kinds of morphisms, ‘pure ones’ (or ‘sharp’) and ‘mixed ones’ (or ‘unsharp’). We represent the pure morphisms as we did throughout this paper:



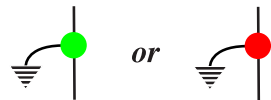
and the mixed ones, for example, as rounded variants of the pure ones:



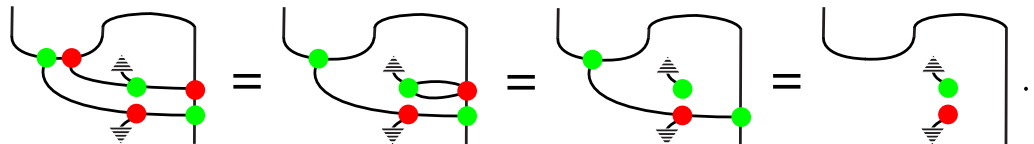
We then introduce a new graphical element  $\Downarrow$ , one for each object, which is coherent with the  $\dagger$ -compact structure, and is subject to an axiom:

$$\begin{array}{c} A \\ | \\ \boxed{f} \\ | \\ A \end{array} = \begin{array}{c} A \\ | \\ \boxed{g} \\ | \\ A \end{array} \quad \text{iff} \quad \begin{array}{c} A \\ | \\ \boxed{f} \\ \Downarrow \end{array} = \begin{array}{c} A \\ | \\ \boxed{g} \\ \Downarrow \end{array} \quad (104)$$

which is valid for all pure morphisms  $f : A \rightarrow B$  and  $g : A \rightarrow C$ . To obtain a precise match with the CPM construction, we also need a *purification axiom* which states that any mixed morphism can be obtained from a pure one by composing the latter with the environment. From (104) it follows that *classical channels*, that is



are idempotent [29]. Here the colour reflects how the classical data was obtained, i.e., in which measurement. This idempotence is in fact the only equation that plays some role in the teleportation protocol, which now goes as follows:



### 12.3. Conditional diagrams [37]

While the previous two approaches represent classical information flow internally, as particular wires in the diagrams, the final alternative presentation of non-determinism ignores the issue of (classical) information flow and focuses on classical correlations that are mediated externally.

Let  $\mathcal{V}$  be a set of formal variables. A *conditional diagram* is a diagram  $\mathfrak{D}$  of the ZX-calculus and, for each Z and X vertex  $v$  in  $\mathfrak{D}$ , an associated subset  $\mathcal{U}_v \subseteq \mathcal{V}$ , possibly empty. A *valuation* is a function  $f : \mathcal{V} \rightarrow \{0, 1\}$ . Each pair  $(\mathfrak{D}, f)$  of a conditional diagram and a valuation determines an *evaluated diagram*  $\mathfrak{D}_f$ , which is obtained from  $\mathfrak{D}$  by modifying the phase  $\alpha$  at each vertex  $v$  as follows:

$$\alpha \mapsto \begin{cases} \alpha & \text{if } \prod_{u \in \mathcal{U}_v} f(u) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and forgetting the sets  $\mathcal{U}_v$ . Each variable corresponds to a two-valued measurement and each valuation  $f$  corresponds to a possible set of measurement outcomes. The evaluated diagram  $\mathfrak{D}_f$  corresponds to the process that occurs when the measurement outcomes corresponding to  $f$

are observed, including both the side-effect of the measurement itself and any other operations which depend classically on its outcome.

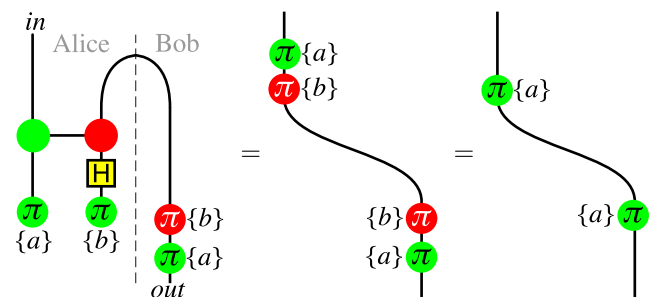
Since each  $\mathfrak{D}_f$  is a diagram of the ZX-calculus, it has an associated linear map,  $D_f$ , as described in section 2.3. We construct a superoperator for  $\mathfrak{D}$  by summing over all possible valuations:

$$\mathbf{D} : \rho \mapsto \sum_f D_f \rho D_f^\dagger.$$

Conditional diagrams can use the same equational rules as the plain ZX-calculus, with the proviso that a rule can only be applied in  $\mathfrak{D}$  if it could be applied to every  $\mathfrak{D}_f$ .

The conditional diagrams approach is essentially a formalization of the informal reasoning demonstrated in section 3.3.1, as the following example will clearly demonstrate.

**Example 12.2.** Let  $\mathcal{V} = \{a, b\}$ , where each variable corresponds to one of the single-qubit measurements comprising the Bell basis measurement in the teleportation protocol. Teleportation protocol can then be formalized as follows:



The crux of the encoding is that the subdiagram

$$\mathfrak{M} = \begin{array}{c} | \\ \pi_{\{a\}} \end{array}$$

denotes the superoperator

$$\rho \mapsto \langle +|\rho|+\rangle + \langle -|\rho|-\rangle,$$

and thus correctly encodes the measurement.






The conditional diagram approach is very well suited to the one-way model, since the quantum part of the system can be very complicated, whereas the classical information flow can usually be taken for granted. For many purposes, for example to translate a one-way pattern to a circuit, we need not evaluate any valuation, and can simply use the equational rules on the conditional diagram directly.

The measurement calculus [30] includes several commands that depend upon on classical bits, here ranged over by  $s$  and  $t$ :

- ${}^s[M_j^\alpha]^t$ —measure qubit  $j$  in the basis  $|0\rangle + e^{(-1)^s i(\alpha + t\pi)}|1\rangle$ .
- $X_j^s$  and  $Z_j^s$ —apply a Pauli X operator (or Z) to qubit  $j$ , if  $s = 1$ ; otherwise do nothing.



Taking  $\mathcal{V}$  to be the set of measured qubits in the pattern, the measurement calculus can be encoded using conditional diagrams according to the table below.

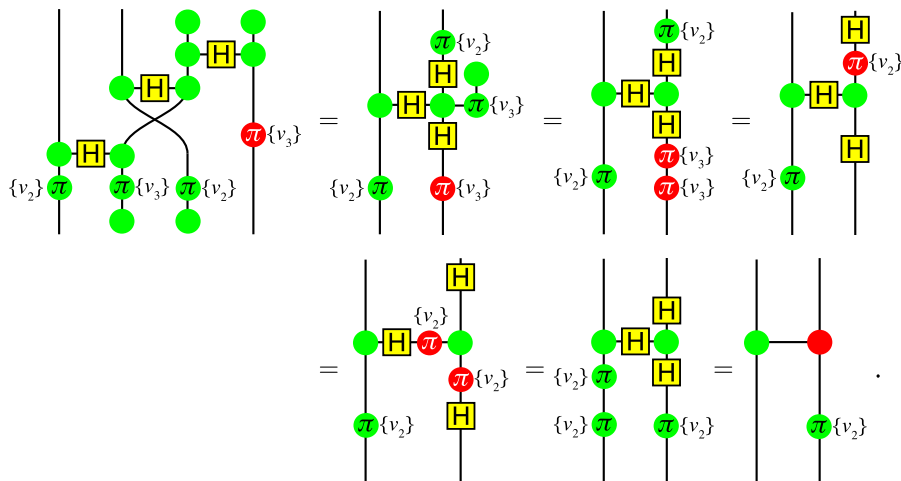
$N_i$	$E_{ij}$	$M_i^\alpha$	$X_i^s$	$Z_i^t$
				

Note that conditional measurement  ${}^s[M_i^\alpha]^t$  is equivalent to the sequence  $M_i^\alpha X_i^s Z_i^t$ , and therefore can be replaced by it.

**Example 12.3.** Consider the pattern

$$X_4^{v_3} Z_4^{v_2} Z_1^{v_2} M_3^0 M_2^0 E_{13} E_{23} E_{34} N_3 N_4.$$

An unreliable quantum software engineer claims that it computes the  $\wedge X$  on its inputs, regardless of the result of the measurements. We can check this claim using equational reasoning on the conditional diagram. Let  $\mathcal{V} = \{v_2, v_3\}$ , corresponding to the outcomes of the measurement of qubits 2 and 3.



Since the final diagram still has the variable  $v_2$  occurring in it, the original claim was false: the result of this pattern depends on the result of the measurement. However, from the diagram we can easily debug the pattern by adding a final correction  $Z_4^{v_2}$  correction at the end. The corrected pattern is

$$Z_4^{v_2} X_4^{v_3} Z_1^{v_2} M_3^0 M_2^0 E_{13} E_{23} E_{34} N_3 N_4.$$

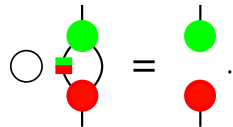
These ideas are developed more fully in [37].

**Remark 12.4.** The notion of conditional diagrams, and their superoperator interpretation, can be easily generalized beyond the minimal setting we have presented here. Variables could take values in an arbitrary set  $A$ —indeed not all variables need have the same set of values—and the modification of the diagram based on the valuation function could be arbitrarily more complicated without changing anything essential. Finally, given an interpretation functor from diagrams into some  $\dagger$ -symmetric monoidal category  $\mathcal{C}$ , then a ‘superoperator’ can be constructed using a suitable semigroup enrichment of  $\mathcal{C}$ .

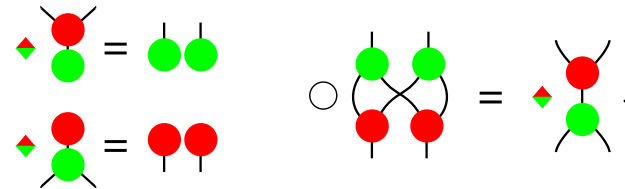
### 13. Conclusion

In this paper we introduced a simple and intuitive—but at the same time universal—graphical calculus for qubits, the ZX-calculus, and have given many example applications. We studied its mathematical underpinning in great detail, in particular:

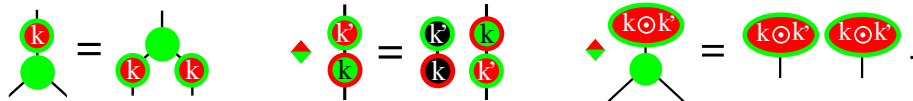
- We obtained a purely diagrammatic characterization of complementarity that extends to observable structures in arbitrary  $\dagger$ -SMCs, in terms of the Hopf law:



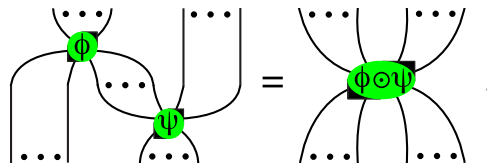
- We identified a strong form of complementarity for observable structures in arbitrary  $\dagger$ -SMCs when the observable structures form a scaled bialgebra:



We identified a number of equivalent alternative formulations:



- We identified a group structure on phases for observable structures in arbitrary  $\dagger$ -SMCs, and proved a generalization of the spider rules, now involving phases:



As already mentioned at the end of the introduction, our results have meanwhile been applied in many contexts, ranging from quantum information and quantum foundations to automated reasoning.

We end the paper by mentioning a number of issues that require further exploration:

- Is there an elegant extension of the ZX-calculus to a ZXY-calculus? Note that this will necessarily involve the dualizers of section 8.2. Would such a ZXY-calculus be different when either modelling **Stab** or **Spek**? (cf example 7.23.)
- What is the precise connection between the stabilizer formalism and our graphical reasoning scheme? (Given that both are adequate tools for studying measurement-based quantum computing.) Is the stabilizer formalism and quantum error correction fully captured by the ZX-calculus?

- Theorem 10.1 adds extra structure with a clear physical interpretation to the phase group: while the elements of  $\mathcal{K}$  may be seen as measurement outcomes, the corresponding cosets can be interpreted as choices of measurements. This may provide the foundation for an axiomatic analysis of non-locality and contextuality. Some work in this direction has already been performed [39].
- Can the ZX-calculus elegantly model many-body states other than graph states, e.g. matrix product states or other states arising in condensed matter physics?
- Does our characterization of complementarity extend in some way or other to observables described by infinite dimensional Hilbert spaces? What is the connection of the above depicted laws with canonical commutation relations?

## Acknowledgments

This work was supported by the authors' respective EPSRC advanced and postdoctoral research fellowships, by the FNRS, by EC FP6 STREP QICS, by an FQXi large grant and by an ONR grant, and we also acknowledge support from Perimeter Institute for Theoretical Physics, which hosted both of the authors. We thank Bertfried Fauser, Prakash Panangaden, Simon Perdrix, Stefano Pironio, Marni Dee Sheppard and the referees for valuable feedback on an earlier version of this paper and to Stephen Brierly and Stefan Weigert for providing the counter-example of remark 9.22.

## References

- [1] Abramsky S and Coecke B 2004 A categorical semantics of quantum protocols *Proc. 19th Annu. IEEE Symp. on Logic in Computer Science (LiCS'04)* (Los Alamitos, CA: IEEE Computer Society Press) (arXiv:quant-ph/0402130)
- [2] Abramsky S and Coecke B 2005 Abstract physical traces *Theory Appl. Categor. **14*** 111–24 ([www.tac.mta.ca/tac/volumes/14/6/14-06abs.html](http://www.tac.mta.ca/tac/volumes/14/6/14-06abs.html))
- [3] Abramsky S and Tzevelekos N 2011 Introduction to categories and categorical logic *New Structures for Physics (Springer Lecture Notes in Physics vol 813)* ed B Coecke (Heidelberg: Springer) pp 3–44
- [4] Amico L, Fazio R, Osterloh A and Vedral V 2008 Entanglement in many-body systems *Rev. Mod. Phys. **80*** 517–76 (arXiv:quant-ph/0703044)
- [5] Baader F and Nipkow T 1999 *Term Rewriting and All That* (Cambridge: Cambridge University Press)
- [6] Baez J and Stay M 2011 Physics, topology, logic and computation: a Rosetta Stone *New Structures for Physics (Springer Lecture Notes in Physics vol 813)* ed B Coecke (Heidelberg: Springer) pp 95–172
- [7] Barrett J 2007 Information processing in general probabilistic theories *Phys. Rev. A **75*** 032304 (arXiv:quant-ph/0508211)
- [8] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett. **70*** 1895–9
- [9] Birkhoff G 1958 von Neumann and lattice theory *Bull. Am. Math. Soc. **64*** 50–6
- [10] Birkhoff G 1961 Lattices in applied mathematics ed R P Dilworth *Lattice Theory, Proc. 2nd Symp. on Pure Mathematics of the American Mathematical Society (April 1959)* (Providence, RI: American Mathematical Society)
- [11] Birkhoff G and von Neumann J 1936 The logic of quantum mechanics *Ann. Math. **37*** 823–43
- [12] Carboni A and Walters R F C 1987 Cartesian bicategories I *J. Pure Appl. Algebra **49*** 11–32
- [13] Cartier P 2006 A primer of Hopf algebras *IHES Preprint*
- [14] Coecke B 2006 Introducing categories to the practicing physicist *What is Category Theory? (Advanced Studies in Mathematics and Logic vol 30)* (Milan: Polimetrica Publishing) pp 45–74 (arXiv:0808.1032)

- [15] Coecke B 2007 De-linearizing linearity: projective quantum axiomatics from strong compact closure *Electron. Notes Theor. Comput. Sci.* **170** 49–72 (arXiv:quant-ph/0506134)
- [16] Coecke B 2008 Axiomatic description of mixed states from Selinger’s CPM-construction *Electron. Notes Theor. Comput. Sci.* **210** 3–13
- [17] Coecke B 2010 Quantum pictorialism *Contemp. Phys.* **51** 59–83 (arXiv:0908.1787)
- [18] Coecke B and Duncan R 2008 Interacting quantum observables ed L Aceto, I Damgrd, L A Goldberg, M M Halldórsson, A Ingólfssdóttir and I Walukiewicz *Proc. 35th Int. Colloquium on Automata, Languages and Programming (ICALP 2008) (Reykjavik, Iceland, 7–11 July 2008) Part II (Lecture Notes in Computer Science* vol 5126) (Heidelberg: Springer) pp 298–310
- [19] Coecke B and Edwards B 2011 Toy quantum categories *Electron. Notes Theor. Comput. Sci.* **270** 29–40 (arXiv:0808.1037)
- [20] Coecke B, Edwards B and Spekkens R W 2011 Phase groups and the origin of non-locality for qubits *Electron. Notes Theor. Comput. Sci.* **270** 15–36 (arXiv:1003.5005)
- [21] Coecke B and Kissinger A 2010 The compositional structure of multipartite quantum entanglement *Proc. 37th Int. Colloquium on Automata, Languages and Programming (ICALP 2010) Part II (Lecture Notes in Computer Science* vol 6199) (Heidelberg: Springer) pp 297–308 (arXiv:1002.2540)
- [22] Coecke B, Moore D J and Wilce A 2000 Operational quantum logic: an overview *Current Research in Operational Quantum Logic: Algebras, Categories and Languages* ed B Coecke, D J Moore and A Wilce (*Fundamental Theories of Physics* vol 111) (Heidelberg: Springer) pp 1–36 (arXiv:quant-ph/0008019)
- [23] Coecke B and Paquette E O 2006 POVMs and Naimark’s theorem without sums *Electron. Notes Theor. Comput. Sci.* **210** 15–31 (arXiv:quant-ph/0608072)
- [24] Coecke B and Paquette E O 2011 Categories for the practicing physicist *New Structures for Physics (Springer Lecture Notes in Physics* vol 813) ed B Coecke (Heidelberg: Springer) pp 173–286 (arXiv:0905.3010)
- [25] Coecke B, Paquette E O and Pavlovic D 2009 Classical and quantum structuralism *Semantic Techniques for Quantum Computation* ed I Mackie and S Gay (Cambridge: Cambridge University Press) pp 26–69 (arXiv:0904.1997)
- [26] Coecke B, Paquette E O and Perdrix S 2008 Bases in diagrammatic quantum protocols *Electron. Notes Theor. Comput. Sci.* **218** 131–52 (arXiv:0808.1037)
- [27] Coecke B and Pavlovic D 2007 Quantum measurements without sums *Mathematics of Quantum Computing and Technology* ed Chen G, Kauffman L and Lomonaco S (London: Taylor and Francis) pp 567–604 (arXiv:quant-ph/0608035)
- [28] Coecke B, Pavlovic D and Vicary J 2008 A new description of orthogonal bases *Mathematical Structures in Computer Science* (Cambridge: Cambridge University Press) to appear (arXiv:0810.0812)
- [29] Coecke B and Perdrix S 2010 Environment and classical channels in categorical quantum mechanics *Proc. 19th EACSL Annu. Conf. on Computer Science Logic (CSL) (Lecture Notes Computer Science* vol 6247) (Heidelberg: Springer) pp 230–44 (arXiv:1004.1598)
- [30] Danos V, Kashefi E and Panangaden P 2007 The measurement calculus *J. ACM* **54** (arXiv:quant-ph/0412135)
- [31] Dieks D G B J 1982 Communication by EPR devices *Phys. Lett. A* **92** 271–2
- [32] Dixon L, Duncan R and Kissinger A *Quantomatic* <http://dream.inf.ed.ac.uk/projects/quantomatic/>
- [33] Dixon L and Duncan R 2009 Graphical reasoning in compact closed categories for quantum computation *Ann. Math. Artif. Intell.* **56** 23–42
- [34] Dixon L and Kissinger A 2010 Open graphs and monoidal theories arXiv:1011.4114
- [35] Duncan R 2006 Types for quantum computing *DPhil Thesis* Oxford University
- [36] Duncan R and Perdrix S 2009 Graph states and the necessity of Euler decomposition *Computability in Europe: Mathematical Theory and Computational Practice (CiE’09) (Lecture Notes in Computer Science* vol 5635) (Heidelberg: Springer) pp 167–77 arXiv:0902.0500
- [37] Duncan R and Perdrix S 2010 Rewriting measurement-based quantum computations with generalised flow *Proc. 37th Int. Colloquium on Automata, Languages and Programming (ICALP 2010) Part II (Lecture Notes in Computer Science* vol 6199) (Heidelberg: Springer) pp 285–96

- [38] Dür W, Vidal G and Cirac J I 2000 Three qubits can be entangled in two inequivalent ways *Phys. Rev. A* **62** 062314
- [39] Edwards B 2010 Phase groups and local hidden variables *Oxford University Computing Laboratory Research Report* RR-10-15 (<http://www.comlab.ox.ac.uk/publications/publication3716-abstract.html>)
- [40] Ehrig H, Ehrig K, Prange U and Taentzer G 2006 *Fundamentals of Algebraic Graph Transformation (Monographs in Theoretical Computer Science)* (Heidelberg: Springer)
- [41] Evans J, Duncan R, Lang A and Panangaden P 2009 Classifying all mutually unbiased bases in Rel arXiv:0909.4453
- [42] Freyd P and Yetter D 1989 Braided compact closed categories with applications to low-dimensional topology *Adv. Math.* **77** 156–82
- [43] Fuchs C A 2001 Quantum foundations in the light of quantum information *Decoherence and its Implications in Quantum Computation and Information Transfer: Proc. NATO Advanced Research Workshop (Mykonos, Greece, 25–30 June 2000)* ed A Gonis and P E A Turchi pp 38–82 (Amsterdam: IOS Press) arXiv:quant-ph/0106166
- [44] Haag R 1992 *Local Quantum Physics: Fields, Particles, Algebras* (Heidelberg: Springer)
- [45] Hardy L 2001 Quantum theory from five reasonable axioms arXiv:quant-ph/0101012
- [46] Jauch J M 1968 *Foundations of Quantum Mechanics* (Reading, MA: Addison-Wesley)
- [47] Joyal A and Street R 1991 The geometry of tensor calculus I *Adv. Math.* **88** 55–112
- [48] Joyal A and Street R 1993 Braided tensor categories *Adv. Math.* **102** 20–78
- [49] Jozsa R 2006 An introduction to measurement based quantum computation *Quantum Information Processing: From Theory to Experiment* ed D G Angelakis, M Christandl, A Ekert, A Kay and S Kulik (Amsterdam: IOS Press) pp 137–58
- [50] Kassel C 1995 *Quantum Groups (Graduate Texts in Mathematics vol 155)* (Heidelberg: Springer)
- [51] Kelly G M and Laplaza M L 1980 Coherence for compact closed categories *J. Pure Appl. Algebr.* **19** 193–213
- [52] Kelly G M and Maclane S 1971 Coherence in closed categories *J. Pure Appl. Algebr.* **1** 97–140
- [53] Kock J 2003 *Frobenius Algebras and 2D Topological Quantum Field Theories* (Cambridge: Cambridge University Press)
- [54] Lack S 2004 Composing PROPs *Theory Appl. Categories* **13** 147–63
- [55] Ludwig G 1985 *An Axiomatic Basis of Quantum Mechanics. 1. Derivation of Hilbert Space* (Heidelberg: Springer)
- [56] Ludwig G 1987 *An Axiomatic Basis of Quantum Mechanics. 2. Quantum Mechanics and Macrosystems* (Heidelberg: Springer)
- [57] Mac Lane S 1998 *Categories for the Working Mathematician* 2nd ed (Heidelberg: Springer)
- [58] Mermin N D 1990 Quantum mysteries revisited *Am. J. Phys.* **58** 731–4
- [59] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
- [60] Pavlovic D 2009 Quantum and classical structures in nondeterministic computation (*Lecture Notes in Computer Science* vol 5494) (Heidelberg: Springer) pp 143–57 (arXiv:0812.2266)
- [61] Penrose R 1971 Applications of negative dimensional tensors *Combinatorial Mathematics and its Applications* (New York: Academic) pp 221–44
- [62] Perdrix S 2005 State transfer instead of teleportation in measurement-based quantum computation *Int. J. Quantum Inf.* **3** 219–23 (arXiv:quant-ph/0402204)
- [63] Pitowski I 1989 *Quantum Probability, Quantum Logic* (Heidelberg: Springer)
- [64] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91
- [65] Raussendorf R, Browne D and Briegel H J 2003 Measurement-based quantum computation on cluster states *Phys. Rev. A* **68** 022312 (arXiv:quant-ph/0301052)
- [66] Rédei M 1997 Why John von Neumann did not like the Hilbert space formalism of quantum mechanics (and what he liked instead) *Stud. History Phil. Mod. Phys.* **27** 493–510
- [67] Schrödinger E 1935 Discussion of probability relations between separated systems *Proc. Camb. Phil. Soc.* **31** 555–63

- [68] Selinger P 2005 Dagger compact closed categories and completely positive maps *Electron. Notes Theor. Comput. Sci.* **170** 139–63 ([www.mathstat.dal.ca/~selinger/papers.html#dagger](http://www.mathstat.dal.ca/~selinger/papers.html#dagger))
- [69] Selinger P 2011 A survey of graphical languages for monoidal categories *New Structures for Physics (Springer Lecture Notes in Physics vol 813)* ed B Coecke (Heidelberg: Springer) pp 289–355
- [70] Selinger P 2010 Autonomous categories in which  $A \simeq A^*$ . Extended abstract *Proc. 7th Int. Workshop on Quantum Physics and Logic (Oxford, 29–30 May)* ([www.mscs.dal.ca/~selinger/papers.html#half twist](http://www.mscs.dal.ca/~selinger/papers.html#half twist))
- [71] Shor P W 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Comput.* **26** 1484–509
- [72] Spekkens R 2007 Evidence for the epistemic view of quantum states: A toy theory *Phys. Rev. A* **75** 032110
- [73] Street R 2007 *Quantum Groups: A Path to Current Algebra* (Cambridge: Cambridge University Press)
- [74] Tadej W and Życzkowski K 2006 A concise guide to complex Hadamard matrices *Open Syst. Inf. Dyn.* **13** 133–77
- [75] Van den Nest M, Dehaene J and De Moor B 2004 Graphical description of the action of local clifford transformations on graph states *Phys. Rev. A* **69** 022316
- [76] Verstraete F and Cirac J I 2004 Valence-bond states for quantum computation *Phys. Rev. A* **70** 060302 (arXiv:quant-ph/0311130)
- [77] Wootters W K and Zurek W 1982 A single quantum cannot be cloned *Nature* **299** 802–3