Interacting Quantum Observables

Bob Coecke and Ross Duncan

Oxford University Computing Laboratory

Abstract. We formalise the constructive content of an essential feature of quantum mechanics: the interaction of complementary quantum observables, and information flow mediated by them. Using a general categorical formulation, we show that pairs of mutually unbiased quantum observables form bialgebra-like structures. We also provide an abstract account on the quantum data encoded in complex phases, and prove a normal form theorem for it. Together these enable us to describe all observables of finite dimensional Hilbert space quantum mechanics. The resulting equations suffice to perform computations with elementary quantum gates, translate between distinct quantum computational models, establish the equivalence of entangled quantum states, and simulate quantum algorithms such as the quantum Fourier transform. All these computations moreover happen within an intuitive diagrammatic calculus.

1 Introduction

Complementary quantum observables such as position and momentum cannot be assigned sharp values at the same time. This fact constitutes the heart of quantum physics. That the self-adjoint operators which characterise these don't commute, motivated the study of non-commutative C^*-algebras, and that their propositional lattices are not distributive resulted in Birkhoff-von Neumann quantum logic. Neither of these axiomatic approaches unveils the true *capabilities* which these complementary observables provide. They merely involve weakening the commutativity/distributivity equation, rendering them essentially useless for any quantum informatic purpose. In this paper we provide an axiomatic account of complementary quantum observables which enables us to tackle problems of actual interest to quantum informatics: algorithm design, identifying the capabilities of multi-partite entanglement, translation between distinct quantum computational models etc. Our starting point is the axiomatisation of quantum observables proposed by Pavlovic and one of the authors in [5] which substantially relied on Carboni and Walters' cartesian bicategories [2]. This notion of quantum observable strongly improves on the one due to Abramsky and one of the authors in [1], the paper which initiated categorical quantum axiomatics, in that it axiomatises quantum observables in terms of dagger symmetric monoidal structure only, allowing for an operational interpretation, a diagrammatic calculus, as well as the 'necessary' higher level of abstraction.[1]

[1] For a detailed discussion of this necessity see [3,12].

L. Aceto et al. (Eds.): ICALP 2008, Part II, LNCS 5126, pp. 298–310, 2008.

Somewhat ironically, while classical structures were crafted to reason about classical control, this paper shows that considering a pair of interacting classical structures—corresponding to complementary quantum observables—are a powerful vehicle to specify and reason about pure quantum states and operations, with many applications. We formalise this notion of complementarity through a set of equations which axiomatise copyability of classical states and the information flow through incompatible classical structures. Surprisingly the relevant equations are almost exactly those of a bialgebra [13], differing only by scalar factors. We show that the axioms of this structure, a *scaled bialgebra*, express the essential features of quantum mechanics in very direct yet usable fashion.

2 Categories of Quantum States and Processes

A †-*symmetric monoidal category* (†-SMC) [12] is a symmetric monoidal category $(\mathbf{C}, \otimes, I)$ together with an identity-on-objects contravariant endofunctor $^\dagger : \mathbf{C} \to \mathbf{C}$ which preserves the monoidal structure. An elementary account of †-SMCs and their graphical representations is in [12]. Well known examples include **Rel**, the category of sets and relations, and **FdHilb**, the category of finite dimensional Hilbert spaces and linear maps.

However quantum states are not vectors in a Hilbert space: they are one-dimensional subspaces. To articulate this fact we will use the word *state* exclusively to refer to such one-dimensional subspaces. Similarly, a non-degenerate observable does not correspond to a basis, but rather a maximal family of mutually orthogonal states. The move from a linear to a projective setting is formalised using a pair of categories, $\mathbf{FdHilb}_p$ and $\mathbf{FdHilb}_{wp}$. The category $\mathbf{FdHilb}_p$ has the same objects as **FdHilb** but its morphisms are equivalence classes of **FdHilb**-morphisms for the congruence

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

This quotient reduces the scalar monoid to a two-element set, hence the capacity for probabilistic reasoning is lost. 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 **FdHilb** and whose morphisms are equivalence classes of **FdHilb**-morphisms for the congruence

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

We regain the absolute values of the inner-product, and thus the probabilistic distance between states.[2] These three categories are related via inclusions:

$$\mathbf{FdHilb}_p \underset{r\in\mathbb{R}^+}{\overset{\twoheadleftarrow}{\hookrightarrow}} \mathbf{FdHilb}_{wp} \underset{\alpha\in[0,2\pi)}{\overset{\twoheadleftarrow}{\hookrightarrow}} \mathbf{FdHilb}$$

2 A detailed categorical account on $\mathbf{FdHilb}_{wp}$ is in [3]; in particular, neither $\mathbf{FdHilb}_p$ nor $\mathbf{FdHilb}_{wp}$ has biproducts, so the approach to measurements taken in [1] will not work here.

We write $|\psi\rangle$ (or rarely ψ) to denote vectors; $\|\psi\rangle\rangle$ denotes a state spanned by this vector. Similarly, $|\sum_i c_i|\,i\,\rangle\rangle$ is the state spanned by vector $\sum_i c_i|\,i\,\rangle$. We take as given a canonical basis for the Hilbert space $\mathbb{C}^n$, which we write $\{|\,i\,\rangle\}_i$. This basis then fixes a canonical observable given by the states $\{\|\,i\,\rangle\rangle\}_i$. The hom-set $\mathbf{FdHilb}_p(\mathbb{C},\mathbb{C}^2)$—that is, the space of linear maps $\mathbb{C} \to \mathbb{C}^2$— corresponds to the the points of the *Bloch sphere*.[3] The unitaries in $\mathbf{FdHilb}_p(\mathbb{C},\mathbb{C}^2)$, i.e. those maps U satisfying $UU^\dagger = U^\dagger U = 1$ correspond to rotations of the Bloch sphere.

3 Classical Structures and the Spider Theorem

A *classical structure* [5] in a †-SMC is an internal cocommutative comonoid $(A, \delta : A \to A \otimes A, \epsilon : A \to \mathrm{I})$ with δ both *isometric* and *Frobenius*, that is,

$$\delta^\dagger \circ \delta = 1_A \qquad \text{and} \qquad \delta \circ \delta^\dagger = (\delta^\dagger \otimes 1_A) \circ (1_A \otimes \delta),$$

respectively. The unit object I canonically comes with classical structure $\lambda_\mathrm{I} : \mathrm{I} \simeq \mathrm{I} \otimes \mathrm{I}$ and 1_I. An orthonormal base $\{\psi_i\}_i$ for Hilbert space $\mathcal{H}$ induces

$$\delta : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H} :: \psi_i \mapsto \psi_i \otimes \psi_i \quad \text{and} \quad \epsilon : \mathcal{H} \to \mathbb{C} :: \psi_i \mapsto 1 \tag{1}$$

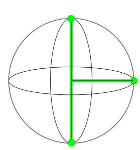
as a classical structure. Conversely, each classical structure in **FdHilb** arises in this way [6]. Hence, classical structure axiomatises the concept of (orthonormal) base in a Hilbert space. Obviously, these classical structures are inherited by $\mathbf{FdHilb}_{wp}$, and passing to $\mathbf{FdHilb}_{wp}$ clarifies what the data which specify a classical structure represent. A state $\|\psi\rangle\rangle$ is *unbiased* for some observable $\{\|\phi_i\rangle\rangle\}_i$ if for all i we have that $|\langle\psi \mid \phi_i\rangle|^2 = 1/\dim(\mathcal{H})$ whenever ψ and ϕ_i are unit vectors. Two observables $\{\|\psi_i\rangle\rangle\}_i$ and $\{\|\phi_i\rangle\rangle\}_i$ are *complementary* whenever $\|\psi_i\rangle\rangle$ is unbiased for $\{\|\phi_j\rangle\rangle\}_j$ for all i.

Proposition 1. *In $\mathbf{FdHilb}_{wp}$ each pair consisting of an observable $\{\|\psi_i\rangle\rangle\}_i$ on a Hilbert space $\mathcal{H}$ and another state $\|\varepsilon\rangle\rangle$ of $\mathcal{H}$ which is unbiased for $\{\|\psi_i\rangle\rangle\}_i$ defines a unique classical structure by setting, for all i,*

$$\delta(\|\psi_i\rangle\rangle) = \|\psi_i \otimes \psi_i\rangle\rangle \qquad \text{and} \qquad |\epsilon(-)| = |\langle\varepsilon, -\rangle|$$

Conversely, all classical structures in $\mathbf{FdHilb}_{wp}$ arise in this way.

The crux to this result is the fact that a set of n base 'vectors' $\{|\psi_i\rangle\}_i$ of a Hilbert space, up to a *common* global phase, is faithfully represented by the $n+1$ 'states' $\{\|\psi_i\rangle\rangle\}_i \cup \{\|\sum_i \psi_i\rangle\rangle\}$. On the Bloch sphere an observable $\{\|\psi_0\rangle\rangle, \|\psi_1\rangle\rangle\}$, e.g. $\{\|0\rangle\rangle, \|1\rangle\rangle\}$, comprises two antipodal points, while $\|\epsilon\rangle\rangle$, e.g. $\|+\rangle\rangle$, lies on the corresponding equator, together making up a T-shape:



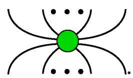
[3] In any monoidal category maps of the type $I \to A$ are called points.

It is standard to interpret the *eigenstates* $\|\psi_i\rangle\rangle$ for an observable $\{\|\psi_i\rangle\rangle\}_i$ as classical data. Hence, in $\mathbf{FdHilb}_{wp}$, the operation δ of a classical structure copies the eigenstates $\|\psi_i\rangle\rangle$ of the observable it is associated with. We can interpret $\|\varepsilon\rangle\rangle$ as the state which uniformly deletes these eigenstates: by unbiasedness the probabilistic distance of each eigenstate $\|\psi_i\rangle\rangle$ to $\|\varepsilon\rangle\rangle$ is equal. Therefore we will refer to δ as (classical) copying and to ϵ as (classical) erasing. A crucial point here is that given an observable there is a choice involved in picking ϵ.

Within graphical calculus for †-SMCs (see [12]) we depict the morphisms δ and ϵ by [green dot with one input, two outputs] and [green dot with one input], and their adjoints, $\delta^\dagger$ and $\epsilon^\dagger$ by [green dot with two inputs, one output] and [green dot with one output], When taking the monoidal structure to be strict—which we will do throughout this paper—classical structures obey the following remarkable theorem [4].[4]

Theorem 1. *Let $f, g : A^{\otimes n} \to A^{\otimes m}$ be two morphisms generated from classical structure (A, δ, ϵ) and the dagger symmetric monoidal structure. If the graphical representation both of f and g is connected then $f = g$.*

Hence, such a morphism only depends on the object A and the number of inputs and outputs. We represent this morphism as an *$n + m$-legged spider*



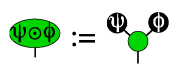
Theorem 1 allows the dots representing δ, ϵ, $\delta^\dagger$ and $\epsilon^\dagger$ to 'fuse' into a single dot, provided all the dots are connected. Note that, conversely, the axioms of classical structure are consequences of this fusing principle.

Classical structure refines the †-compact structure which was used in [1,12], provided the latter is self-dual. Graphical reasoning in compact structure by 'yanking' is subsumed by reasoning in terms of the above 'spider theorem'. This will become clear in the first example of §6.3. We can define the *conjugate* $f_* : A \to B$ of a morphism $f : A \to B$ relative to classical structures $(A, \delta_A, \epsilon_A)$ and $(B, \delta_B, \epsilon_B)$ to be $f_* := (1_B \otimes \eta_A^\dagger) \circ (1_B \otimes f^\dagger \otimes 1_A) \circ (\eta_B \otimes 1_A)$ where $\eta_X := \delta_X \circ \epsilon_X^\dagger$. In **FdHilb** the linear function f_* is obtained by conjugating the entries of the matrix of f when expressed in the classical structure bases. The *dimension* of A is $\dim(A) := \eta_A^\dagger \circ \eta_A$ represented graphically by a circle.

4 A Generalised Spider Theorem and Abstract Phase Data

Let (A, δ, ϵ) be a classical structure in a †-SMC. On *points* $\psi, \phi : I \to A$ we define

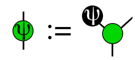
$$\psi \odot \phi = \delta^\dagger \circ (\psi \otimes \phi) \qquad \text{i.e.}$$



[4] Similar results are known for concrete dagger Frobenius algebras, e.g. 2D topological quantum field theories, as well as in more abstract categorical settings [11].

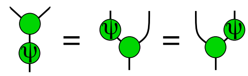
Since $(A, \delta^\dagger, \epsilon^\dagger)$ forms a commutative monoid, this operation is immediately associative and commutative, with unit $\epsilon^\dagger$. Now define

$$\Lambda : \mathbf{C}(I, A) \to \mathbf{C}(A, A) :: \psi \mapsto \delta^\dagger \circ (\psi \otimes 1_A) \qquad \text{i.e.}$$



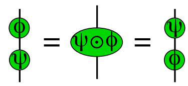
From the properties of $\delta^\dagger$ it immediately follows that Λ is a homomorphism of monoids, and that for every ψ

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



Since $\odot$ is commutative, we also have

$$\Lambda(\psi) \circ \Lambda(\phi) = \Lambda(\phi) \circ \Lambda(\psi) \qquad \text{i.e.}$$

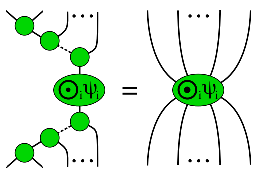


and since $\Lambda(\psi)^\dagger = (\psi^\dagger \otimes 1_A) \circ \delta$, the spider theorem yields $\Lambda(\psi)^\dagger = \Lambda(\psi_*)$. Now let $\delta_n : A \to A^{\otimes n}$ be defined by the recursion $\delta_0 = \epsilon$, $\delta_1 = 1_A$ and $\delta_n = \delta \circ (\delta_{n-1} \otimes 1_A)$.

Theorem 2. *Let $f : A^{\otimes n} \to A^{\otimes m}$ be a morphism generated from classical structure (A, δ, ϵ), points $\psi_i : I \to A$ (not necessarily all distinct), and dagger symmetric monoidal structure. If the graphical representation of f is connected then*

$$f = \delta_m \circ \Lambda\Big(\bigodot_i \psi_i\Big) \circ \delta_n^\dagger . \tag{2}$$

This is a strict generalisation of Theorem 1: besides the number of inputs and outputs there is now also the *product of all points* which distinguishes classes of equal diagrams. We obtain a *decorated spider*:



In graphical terms, Theorem 2 allows arbitrary decorated dots of the same colour to 'fuse' together provided we 'multiply their decorations'.

In $\mathbb{C}^n$, consider $|\psi\rangle = \sum_i c_i |\, i\,\rangle$; when written in the basis fixed by (δ, ϵ), $\Lambda(\psi)$ consists of the diagonal $n \times n$ matrix with $c_1, \ldots, c_n$ on the diagonal. Hence, $\Lambda(\psi)$ is unitary, upto a normalisation factor, if and only if $\|\psi\rangle\rangle$ is unbiased for $\{\|1\rangle\rangle, \ldots, \|n\rangle\rangle\}$. This fact admits generalisation to arbitrary †-SMCs.

Definition 1. We call $\psi : I \to A$ *unbiased relative to* δ if $\Lambda(\psi)$ is unitary.

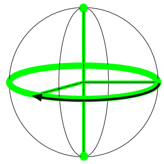
Proposition 2. *The set of points which are unbiased relative to a classical structure forms a group under $\odot$ with $(-)_*$ as the inverse.*

For ψ unbiased relative to δ, by Theorem 2 and Proposition 2, we have

$$= \big(\Lambda(\psi) \otimes \Lambda(\psi)\big) \circ \delta \circ \Lambda(\psi)^\dagger \qquad \text{and}$$

$$= \epsilon \circ \Lambda(\psi)^\dagger$$

and again by the generalised spider theorem it then follows that these morphisms define a classical structure. We call it a *phase shift* of (A, δ, ϵ). In $\mathbb{C}^2$, these phased variants to the classical structure $\{\|0\rangle\!\rangle, \|1\rangle\!\rangle, \|+\rangle\!\rangle\}$ (cf. Proposition 1) are those obtained by varying the choice of $\|\varepsilon\rangle\!\rangle$ on the equator of the Bloch sphere:



.

The states which are unbiased relative to $\{\|0\rangle\!\rangle, \|1\rangle\!\rangle\}$ are of the form $\|+_\theta\rangle\!\rangle := \big||0\rangle + e^{i\theta}|1\rangle\big\rangle$ so form a family parameterised by a phase θ. In particular, we have $\|+_{\theta_1}\rangle\!\rangle \odot \|+_{\theta_2}\rangle\!\rangle = \|+_{\theta_1+\theta_2}\rangle\!\rangle$, that is, the operation $\odot$ boils down to *adding up* phases modulo 2π, which is an abelian group with minus as inverse.

5 Complementary Observables as Scaled Bialgebras

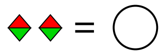
The goal of this section is to show that each pair of complementary observables in $\mathbf{FdHilb}_{wp}$ defines a *scaled bialgebra*. In the next section we will then use this scaled algebra structure together with the generalised spider theorem for phase data to reason about quantum informatics. First we define and study an abstract notion of complementary observables. We then derive a general scaled bialgebra law in categories with 'enough points' such as **FdHilb**. This result then carries over to $\mathbf{FdHilb}_{wp}$ where it takes a much simpler form.

5.1 Complementary Classical Structures (CCSs)

In eq.(1) we described classical structures in **FdHilb** as maps which copy base vectors, and hence also the corresponding states in $\mathbf{FdHilb}_{wp}$. We introduce an abstract counterpart to these 'copy-able' points. We assume as given a classical structure (A, δ, ϵ) in a †-SMC.

Recall that if a †-SMC has a classical structure on an object A then the monoidal subcategory generated by A is †-compact, and hence we can define the *dimension* of A by $\dim(A) = \epsilon \circ \delta^\dagger \circ \delta \circ \epsilon^\dagger$.[5] For brevity, we define $D = \dim(A)$. We will, in addition, assume the existence of a self-adjoint scalar $\sqrt{D}$, which we we denote graphically as . As the notation suggests, $\sqrt{D}$ satisfies

$$\sqrt{D} \otimes \sqrt{D} = D = \dim(A) \qquad \text{or, graphically:}$$

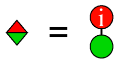


.

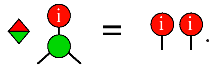
Notation. We represent all the points $a : I \to A$ which are unbiased with respect to (A, δ, ϵ) by dots of the same green (light grey) colour used before. Those points which are 'copied' by δ in the sense of the definition below we mark by a different colour, here red, or darker grey. Any other points are marked in black. In light of the special role played by unbiased points, we will use the spider notation only for these.

[5] One can show that $\dim(A)$ does not depend on the choice of classical structure.

Definition 2. *We call a point* $a_i : I \to A$ classical relative to (A, δ, ϵ) *if both* $\sqrt{D} = \epsilon \circ a_i$ *and* $\sqrt{D} \cdot (\delta \circ a_i) = a_i \otimes a_i$ *hold, that is, graphically,*



and

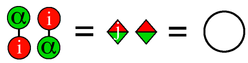


The classical points for a classical structure in $\mathbf{FdHilb}_{wp}$ are of course the states $\{\|\psi_i\rangle\rangle\}_i$ of Proposition 1.

The abstract conception of a classical point allows the concrete notion of unbiasedness to be derived from the abstract formulation of Definition 1:

Lemma 1. *If* $a_i : I \to A$ *is classical and* $\alpha : I \to A$ *unbiased for* (A, δ, ϵ) *then*

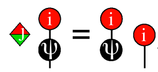
$$(\alpha^\dagger \circ a_i) \cdot (\alpha^\dagger \circ a_i)^\dagger = D \qquad \text{i.e.}$$



The classical points are "eigenvectors" in a suitable sense:

Lemma 2. *If* $a_i : I \to A$ *is classical for* (A, δ, ϵ) *and* $\psi : I \to A$ *arbitrary then*

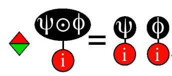
$$\sqrt{D} \cdot (\Lambda(\psi) \circ a_i) = (\psi_*^\dagger \circ a_i) \cdot a_i \qquad \text{i.e.}$$



The monoid multiplication on points carries over to scalars:

Lemma 3. *Let* $a_i : I \to A$ *be classical and* $\psi, \phi : I \to A$ *arbitrary then*

$$\sqrt{D} \cdot (a_i^\dagger \circ (\psi \odot \phi)) = (a_i^\dagger \circ \psi) \cdot (a^\dagger \circ \phi) \qquad \text{i.e.}$$



Remark 1. The reader may find the scalar factors in the above equations mysterious, not to say vexing. But recall that in **FdHilb** the equation $\left|\epsilon^\dagger\right| = \sqrt{D}$ is required to satisfy the comonoid laws; this scalar factor reappears here.[6]

Definition 3. Two classical structures $(A, \delta_X, \epsilon_X)$ and $(A, \delta_Z, \epsilon_Z)$ in a †-SMC are called *complementary* if they obey the following rules:

- whenever $z_i : I \to A$ is classical for (δ_X, ϵ_X) it is unbiased for (δ_Z, ϵ_Z);
- whenever $x_j : I \to A$ is classical for (δ_Z, ϵ_Z) it is unbiased for (δ_X, ϵ_X);
- $\epsilon_X^\dagger$ is classical for (δ_Z, ϵ_Z) and $\epsilon_Z^\dagger$ is classical for (δ_X, ϵ_X).

We abbreviate *complementary classical structure* as CCS.

Notation. The reason that we refer to the classical points of $(A, \delta_X, \epsilon_X)$ by z_i, and vice versa, is because z_i is unbiased to (δ_Z, ϵ_Z) and hence can participate in the generalised spider theorem for the classical structure (δ_Z, ϵ_Z).

For any non-degenerate quantum observable we can find a pair of complementary classical structures in $\mathbf{FdHilb}_{wp}$ merely by picking $\|\varepsilon\rangle\rangle$ for one observable from among the eigenstates of the other observable.

[6] An alternative would be to replace $(\epsilon \otimes 1_{\mathcal{H}}) \circ \delta = 1_{\mathcal{H}}$ with $(\epsilon \otimes 1_{\mathcal{H}}) \circ \delta = \frac{1}{\sqrt{D}} 1_{\mathcal{H}}$.

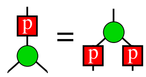
5.2 Derivation of the Scaled Bialgebra Law from Abstract Bases

Definition 4. A set of points $\{a_i\}_i$ is a *basis* for an object A if for all $f, g : A \to B$, if $f \circ a_i = g \circ a_i$ for all a_i, then $f = g$. A basis is *classical*, or *unbiased*, with respect to some classical structure (A, δ, ϵ) if its elements are respectively classical, or unbiased, with respect to this structure. An unbiased basis is called *closed* if for all a_i, a_j there exists a_k such that $a_i \odot a_j = a_k$ and $a_0 = \epsilon^\dagger$. We say that a †-SMC has *monoidal bases* when, for each basis $\{a_i\}_i$ for A, and each basis $\{b_j\}_j$ for B, the set $\{a_i \otimes b_j\}_{ij}$ is a basis for $A \otimes B$.

An immediate consequence of this definition is that whenever b is an element of a closed unbiased basis $\{b_i\}_i$, then $\Lambda(b)$ is a permutation on the set $\{b_i\}_i$. Further, by Lemma 2 every classical point is an eigenvector of $\Lambda(b)$.

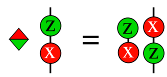
Lemma 4. *Let $\{a_i\}_i$ be a classical basis for A suppose $p : A \to A$ acts as a permutation on this set; then*

$$(p \otimes p) \circ \delta = \delta \circ p \qquad \text{i.e.}$$



Lemma 5. *Let (δ_X, ϵ_X), (δ_Z, ϵ_Z) be CCSs, let x be in a closed classical basis of (δ_Z, ϵ_Z) and let z be unbiased for (δ_Z, ϵ_Z), then*

$$\sqrt{D} \cdot (\Lambda^X(x) \circ \Lambda^Z(z)) = (x^\dagger \circ z) \cdot (\Lambda^Z(z) \circ \Lambda^X(x)) \quad \text{i.e.}$$



The Pauli matrices provide an example of these commutation relations.

Lemma 6. *Let (δ_Z, ϵ_Z) and (δ_X, ϵ_X) be CCSs and let U_Z denote all the unbiased points and C_Z a basis of classical points for (δ_Z, ϵ_Z). Suppose $x \in C_Z$ and let $\mathsf{X} = \Lambda^X(x)$. If C_Z is closed under $\odot_X$ then:*

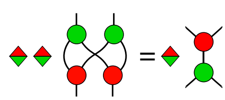
- X *is a permutation on C_Z;*
- X *is an automorphism on U_Z such that*

$$\mathsf{X} \circ (\alpha \odot_Z \beta) = (\mathsf{X} \circ \alpha) \odot_Z (\mathsf{X} \circ \beta); \quad , \quad \mathsf{X} \circ \epsilon_Z^\dagger = \epsilon_Z^\dagger \quad \text{and} \quad (\mathsf{X} \circ \alpha)^{-1} = \mathsf{X}^\dagger \circ \alpha^{-1}.$$

Corollary 1. *$(C_Z, \odot_X)$ is an abelian group with a group action on U_Z defined by $(x, z) \mapsto \Lambda^X(x) \circ z$.*

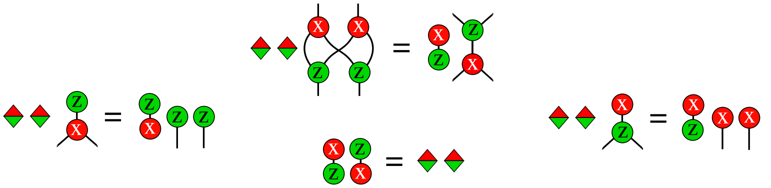
Lemma 7. *Consider a †-SMC with monoidal bases and let σ be the monoidal symmetry. Let $(A, \delta_X, \epsilon_X)$ and $(A, \delta_Z, \epsilon_Z)$ be CCSs with classical bases $\{z_j\}_j$ and $\{x_i\}_i$; $\{x_i\}_i$ is closed if and only if*

$$D \cdot (\delta_X^\dagger \otimes \delta_X^\dagger) \circ (1_A \otimes \sigma \otimes 1_A) \circ (\delta_Z \otimes \delta_Z) = \sqrt{D} \cdot \delta_Z \circ \delta_X^\dagger \quad \text{i.e.}$$



Corollary 2. *In the above situation $\{x_i\}_i$ is closed if and only if $\{z_i\}$ is.*

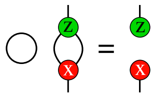
Theorem 3. *Let (δ_X, ϵ_X) and (δ_Z, ϵ_Z) be CCSs with closed bases including the points z and x respectively. Then, graphically,*



(3)

We call the morphisms obeying eq.(3) *a 'scaled bialgebra'.*

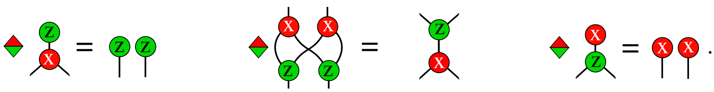
Proposition 3. *If* (δ_X, ϵ_X) *and* (δ_Z, ϵ_Z) *form a scaled bialgebra then*



i.e. it is a 'scaled Hopf algebra' with $\dim(A) \cdot 1_A$ *as its 'antipode'.*

5.3 Complementary Classical Observables in $\mathbf{FdHilb}_{wp}$

Classical structures in **FdHilb** 'are' bases [6] so complementary pairs of bases which satisfy the closedness condition of Definition 4 induce scaled bialgebras in the sense of Theorem 3. These scaled bialgebra laws carry over to the CCSs in $\mathbf{FdHilb}_{wp}$ consisting of the states spanned by the basis vectors. Moreover, in $\mathbf{FdHilb}_{wp}$, since all scalars are positive reals, all scalars in eqs.(3) coincide, so cancellation simplifies eqs.(3) to



(4)

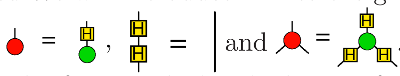
Conversely, any pair of complementary observables yields a family of CCSs in $\mathbf{FdHilb}_{wp}$ mediated by a group of permutations on the respective sets of classical states, and one can always construct a corresponding underlying family of CCSs in **FdHilb**. What we so far failed to prove is that in general we can always construct a corresponding underlying family of 'closed' CCSs. However: **(i)** CCSs in **FdHilb** on $\mathbb{C}^2$ and $\mathbb{C}^3$ 'are' closed; **(ii)** CCSs can be chosen to be closed for all (to us) known constructions of mutually unbiased bases (e.g. [10]); **(iii)** we constructed closed CCSs on $\mathbb{C}^n$ in $\mathbf{FdHilb}_{wp}$ for all n. Hence for all practical situations involving complementary observables eq.(4) hold. We conjecture that closed CCSs can be derived from any pair of mutually unbiased observables.[7]

6 Applications and Examples in Quantum Informatics

Inevitably, the examples from this field are constructed from the ubiquitous qubit i.e. $\mathbb{C}^2$. Take the 'green' classical structure (δ_Z, ϵ_Z) as in eq.(1) for $\{|0\rangle, |1\rangle\}$. The unbiased points for (δ_Z, ϵ_Z) are of the form $|\alpha_Z\rangle = |0\rangle + e^{i\alpha}|1\rangle$, and $|\alpha_Z\rangle \odot_Z$

[7] The study of mutually unbiased bases is an active area of research; characterisation of the maximal number of mutually unbiased bases is one of the important open problems in quantum informatics.

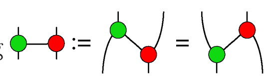
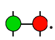
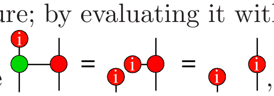
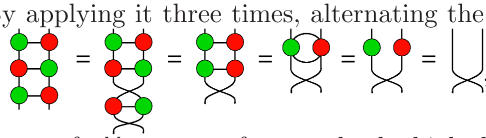
$|\beta_Z\rangle = |\alpha + \beta_Z\rangle$. Further, $\Lambda^Z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$, in particular, $\Lambda^Z(\pi) = \mathsf{Z}$. Notice that $\epsilon_Z^\dagger = |0\rangle + |1\rangle$ and $|\pi_Z\rangle = |0\rangle - |1\rangle$ form a basis, which is closed and unbiased with respect to (δ_Z, ϵ_Z) and define a complementary 'red' classical structure (δ_X, ϵ_X). The unbiased points for (δ_X, ϵ_X) have the form $|\theta_X\rangle = \sqrt{2}(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle)$ and $\Lambda^X(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$, in particular, $\Lambda^Z(\pi) = \mathsf{X}$. We have $\mathsf{Z} \circ |\theta_X\rangle = |-\theta_X\rangle$, and, upto a global phase, $\mathsf{X} \circ |\alpha_Z\rangle = |-\alpha_Z\rangle$. In the language of Lemma 6 we have: if $|C_Z| = 2$, then $(C_Z, \odot_X)$ is the symmetric group S_2, its unique non-identity element X is self-adjoint, and for $\alpha \in U_Z$ we have $\mathsf{X} \circ \alpha = \alpha_*$ i.e. X assigns the inverses for the group U_Z.

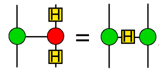
For some of the examples below it will also be convenient to explicitly have the unitary operation which changes the green dots into red dots, that is, concretely, the unitary operation which establishes the corresponding change of basis. In the case of (δ_Z, ϵ_Z) and (δ_X, ϵ_X) given above, the two structures are connected via the familiar Hadamard map H. As well as being unitary, $H = H^\dagger$ so this map is particularly well behaved.We will introduce H into the graphical language with the following equations .

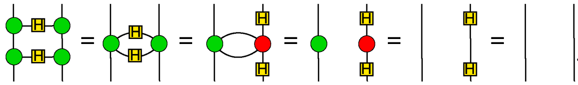
Below we disregard scalar factors which only distract from the essential point.

6.1 Quantum Gates, Circuits, and Algorithms

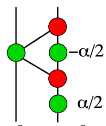
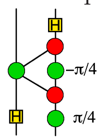
Above we introduced 1-qubit unitaries $\Lambda^Z(\alpha)$ and $\Lambda^X(\beta)$ corresponding to rotations in the X-Y and the Y-Z planes respectively; these suffice to represent all 1-qubit unitaries, and their basic equational properties follow from the various lemmas introduced in the preceding sections. We demonstrate how to define the $\wedge\mathsf{X}$ and $\wedge\mathsf{Z}$ gates, and prove two elementary equations involving them. The addition of these gates will provide a computationally universal set of gates.

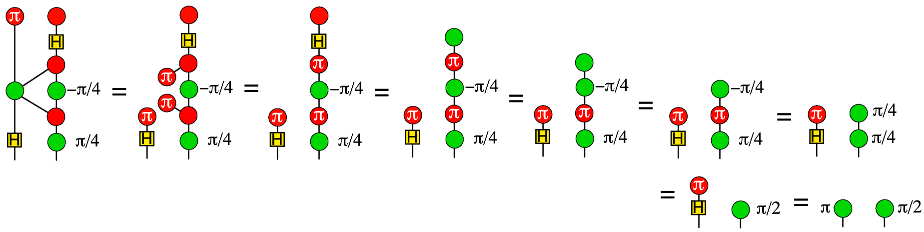
Example 1 ($\wedge$X gate). Setting  one verifies by concrete calculation that $\wedge\mathsf{X} =$ . We can also give an abstract proof . Let $|i\rangle$ be a classical point for the green classical structure; by evaluating it with an input to its control qubit (the green end) we have , which for $|i\rangle = |0_X\rangle$ is the identity, and in the binary case, for $|i\rangle = |1_X\rangle$, is the unique operation X. By applying it three times, alternating the target and control input, we obtain, , i.e. σ. while this is a well-known property of $\wedge\mathsf{X}$, our proof uses only the bialgebra structure hence it will hold in much greater generality than just for qubits.

Example 2 (∧Z gate). One can derive the ∧Z from that of ∧X by augmenting the target qubit of the ∧X with H gates i.e. = . We have that

$\wedge Z \circ \wedge Z = 1$ since .

Example 3 (An algorithm : the quantum Fourier transform). The quantum Fourier transform is one of the most important quantum algorithms, lying at the centre of Shor's famous factoring algorithm. The equations we have enable this algorithm to be simulated in the diagrammatic language. Unlike the preceding examples, here we require the interaction between the two phase groups.

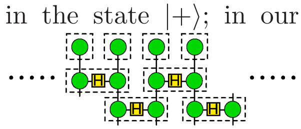
In our language the $\wedge Z_\alpha$ gate is  and the circuit  involving it realises the quantum Fourier transform for 2 qubits. The algorithm can be simulated graphically, as shown below:

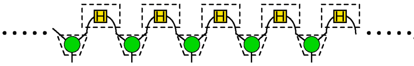
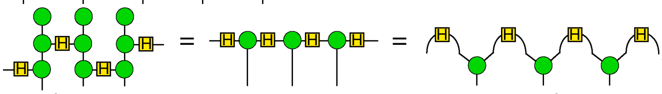


This example makes use of classical values coded as quantum states to control the interference of phases: this is the archetypal behaviour of quantum algorithms.

6.2 Multi-partite Entanglement

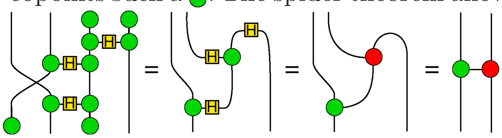
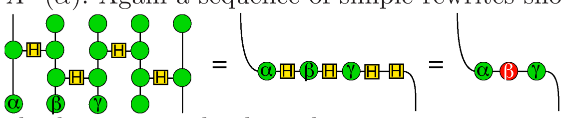
In our graphical language, a quantum state is nothing more than a circuit with no inputs; output edges correspond to the individual qubits making up the state. The interior of the diagram, i.e. its graph structure, describes how these qubits are related. Hence this notation is ideal for representing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

Example 4. The cluster states used in measurement-based quantum computing, can be prepared in several ways; the graphical calculus provides short proofs of their equivalence. For example, the original scheme describes a ∧Z interaction between qubits initially prepared in the state $|+\rangle$; in our notation this is $|0_Z\rangle$, or . So 1D cluster arises as  where the boxes delineate the individual $|+\rangle$ preparations and ∧Z operations. Alternatively, the cluster state can be prepared by fusion of states of the form $|0+\rangle + |1-\rangle$. Our $\delta_Z^\dagger$ is in fact this fusion operation, so a 1D cluster arises as

. Using the spider theorem, these are equivalent . Ongoing work seeks to classify multipartite entangled states in terms of their graphical representatives, and to formalises general matrix product states.

6.3 Properties of Quantum Computational Models

Our formalism axiomatises two key features of quantum mechanics: the underlying monoidal structure and the interaction of complementary observables. Furthermore it is a semantic, which is to say *extensional*, framework which makes it ideal for unifying various approaches to quantum computation. E.g. we can demonstrate equivalence between different quantum computational models.

Example 5 (Verifying one-way quantum computations). We show how to verify some example programs for the one-way model, taken from [7], by translation to equivalent quantum circuits. Post-selected qubit measurements[8] can be represented by copoints such a . The spider theorem allows the post-selected one-way program  implementing a ∧X operation upon its inputs to be rewritten to a ∧X gate in no more than two steps . Now recall that any single qubit unitary map U has an Euler decomposition as such that $U = Z_\alpha X_\beta Z_\gamma$. In our notation this is $Z_\alpha = \Lambda^Z(\alpha)$ and $X_\alpha = \Lambda^X(\alpha)$. Again a sequence of simple rewrites shows that the one-way program  to compute such a unitary indeed computes the desired map.

References

1. Abramsky, S., Coecke, B.: A categorical semantics of quantum protocols. In: Abramsky, S., Coecke, B. (eds.) Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LiCS). IEEE Computer Science Press, Los Alamitos (2004); Abstract physical traces. Theory and Applications of Categories 14, 111–124 (2005)
2. Carboni, A., Walters, R.F.C.: Cartesian bicategories I. Journal of Pure and Applied Algebra 49, 11–32 (1987)
3. Coecke, B.: De-linearizing linearity: projective quantum axiomatics from strong compact closure. ENTCS 170, 49–72 (2007)

[8] Classical structures were initially introduced in [5] to represent classical control structure so this example can easily be extended with the required unitary corrections.

4. Coecke, B., Paquette, E.O.: POVMs and Naimark's theorem without sums (2006) (to appear in ENTCS), arXiv:quant-ph/0608072
5. Coecke, B., Pavlovic, D.: Quantum measurements without sums. In: Chen, G., Kauffman, L., Lamonaco, S. (eds.) Mathematics of Quantum Computing and Technology, pp. 567–604. Taylor and Francis, Abington (2007)
6. Coecke, B., Pavlovic, D., Vicary, J.: Dagger Frobenius algebras in FdHilb are bases. Oxford University Computing Laboratory Research Report RR-08-03 (2008)
7. Danos, V., Kashefi, E., Panangaden, P.: The measurement calculus. Journal of the ACM 54(2) (2007), arXiv:quant-ph/0412135
8. Joyal, A., Street, R.: The Geometry of tensor calculus I. Advances in Mathematics 88, 55–112 (1991)
9. Kelly, G.M., Laplaza, M.L.: Coherence for compact closed categories. Journal of Pure and Applied Algebra 19, 193–213 (1980)
10. Klappenecker, A., Rötteler, M.: Constructions of mutually unbiased bases. LNCS, vol. 2948, pp. 137–144. Springer, Heidelberg (2004)
11. Kock, J.: Frobenius Algebras and 2D Topological Quantum Field Theories. In: Composing PROPs. Theory and Applications of Categories, vol. 13, pp. 147–163. Cambridge University Press, Cambridge (2003)
12. Selinger, P.: Dagger compact closed categories and completely positive maps. ENTCS, 170, 139–163 (2005), `www.mathstat.dal.ca/~selinger/papers.htmldagger`
13. Street, R.: Quantum Groups: A Path to Current Algebra, Cambridge UP (2007)