Models of Quantum Algorithms in Sets and Relations

William Zeng

Department of Computer Science, University of Oxford, Oxford, UK
`william.zeng@cs.ox.ac.uk`

Abstract. We construct abstract models of blackbox quantum algorithms using a model of quantum computation in sets and relations, a setting that is usually considered for nondeterministic classical computation. This alternative model of quantum computation (QCRel), though unphysical, nevertheless faithfully models its computational structure. Our main results are models of the Deutsch-Jozsa, single-shot Grovers, and GroupHomID algorithms in QCRel. These results provide new tools to analyze the semantics of quantum computation and improve our understanding of the relationship between computational speedups and the structure of physical theories. They also exemplify a method of extending physical/computational intuition into new mathematical settings.

Keywords: quantum algorithms · programming semantics · groupoids · category theory

1 Introduction

Despite almost two decades of research, we still seek new and useful quantum algorithms. This is of interest in cases where the meaning of useful ranges from "able to generate experimental evidence against the extended Church-Turing thesis" to "commercially viable". Better languages, frameworks, and techniques for analyzing the structure of quantum algorithms will aid in these attempts. One such programme initiated by Abramsky, Coecke, et al. de-emphasizes the role of Hilbert spaces and linear maps and instead focuses on topological flows of information within quantum-like systems [1,3,6]. This approach captures all the familiar structure of quantum computation from teleportation to quantum secret-sharing and locates the particular quantum setting of Hilbert spaces as an instance of more general abstract process theories [4,5]. Recent work has developed the presentation and verification of quantum algorithms such as the Deutsch-Jozsa and Grover algorithms, and the quantum Fourier transform [11] in terms of these abstract process theories, finding new generalizations and algorithms [21,22].

Having grasped the abstract structure at play in the protocols and algorithms of quantum computation, we can conceive of modelling quantum computation in settings other than Hilbert spaces and linear maps. There are two main thrusts that make this investigation, the subject of this paper, interesting. The

first is to further analyze the structure of quantum computation, advancing our understanding of the relationship between computational speedups and the structure of physical theories. We use the QCRel model defined here to analyze some example quantum algorithms as non-deterministic classical algorithms while preserving their query-complexity (and, in fact, all their abstract structure). The second thrust regards the insights that become available by extending physical/computational intuition into new areas of mathematics. While other toy models of a relational flavor for quantum mechanics have been proposed [9,12,18,20], and some even discuss protocols [15], these works have not developed the structures necessary to model quantum algorithms.

The next section of this paper constructs our chosen model of quantum information. This is the setting of sets and relations, rather than Hilbert spaces and linear maps, and it is introduced by rephrasing the axioms of quantum mechanics. Section 3 introduces a graphical notation for analyzing processes in this setting. Sections 4-9 present the novel contributions of this paper: relational models of unitary oracles, the Deutsch-Jozsa algorithm, the single-shot Grover's algorithm, and the group homomorphism identification algorithm.

2 The Model of Quantum Computation in Relations

We begin by defining the key components of quantum computation in this new setting, e.g. systems, states, bases, etc. The following definitions are motivated by examples from [1,5,10] that are summarized in [4,14], whose general theorems prove useful. To avoid distracting repetition of notation, we use generic terminology to refer to the relational setting within this paper. For example *system* is intended to mean *relational system*, i.e. a set. When we wish to refer to the quantum setting we explicitly denote this e.g. *quantum system* refers to a finite dimensional Hilbert space.

Axiom 1. *A* system *is a set H with* states $|\psi\rangle$ *given by subsets $\psi \subseteq H$.*

Each state in our notation is a boolean column vector written as a labelled ket, to follow the convention in quantum mechanics where states are complex valued column vectors as in the following example.

Example 1. Consider a three element system $\{0, 1, 2\}$, the relation $R = \{(0,0),(0,2),(1,1)\}$ and the state $|\psi\rangle = \{0\}$. In terms of boolean matrices and vectors the composition $R \circ |\psi\rangle$ is written as:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \tag{1}$$

The state $|\psi \vee \phi\rangle$ has elements in the union of sets ψ and ϕ. We often use $|\psi\rangle$ to mean the relation $\{\bullet\} \rightarrow H$ that relates the singleton set to all the elements in ψ.

Axiom 2. *A* composite system H *of n subsystems is given by the Cartesian product so that $H = H_1 \times ... \times H_n$.* Composite states *are any subset of H.*

Definition 2. *For a relation $R : A \rightarrow B$ from set A to B, the* converse relation *is denoted $R^{-1} : B \rightarrow A$ where for $x \in A$ and $y \in B$, xRy if and only if $yR^{-1}x$.*

The converse replaces the †-adjoint in quantum mechanics. This leads to:

Definition 3. *A relation $R : H_1 \rightarrow H_2$ is* unitary *if and only if $R \circ R^{-1} = id_{H_1}$ and $R^{-1} \circ R = id_{H_2}$, where $Q \circ R$ means Q after R.*

This is the relational analog to the usual unitarity of linear maps in quantum mechanics and has an obvious interpretation:

Corollary 4. *Relations are unitary if and only if they are bijections.*

Axiom 3. Evolution *of systems is given by unitary relations.*

This means that states of system A can evolve to states of system B if and only if there is a bijection between them. Note that this implies that there do not exist physical evolutions between systems of different cardinality.

Definition 5. *For a state $|\psi\rangle : \{\bullet\} \rightarrow H$, denote its relational converse as $\langle\psi| : H \rightarrow \{\bullet\}$ called its* effect.

A state preparation followed by an effect amounts to an experiment with a post-selected outcome. Effects are maps to $\{\bullet\}$ that return whether the outcome state $|\psi\rangle$ is possible. We give an example to illustrate:

Example 6. The preparation of the state $|\phi\rangle$ followed by a post-selected measurement of the effect $\langle\psi|$ is given by the relation

$$\langle\psi|\phi\rangle := \langle\psi| \circ |\phi\rangle : \{\bullet\} \rightarrow H \rightarrow \{\bullet\}$$

This is either the identity relation that we interpret to mean a measurement outcome of $\langle\psi|$ is *possible*, or it is the empty relation that we interpret to mean the measurement outcome $\langle\psi|$ is *impossible*. It is clear that the outcome $\langle\psi|$ is possible if there exists some element of H in both ψ and ϕ. Otherwise it is impossible. In this sense our relational quantum computation is a deterministic model of quantum computation.

This interpretation allows us to define a generalized version of the Born rule[1] to describe measurement in our model.

---

[1] In quantum theory, the Born rule gives the probability of measuring the outcome state $|\psi\rangle$ following preparation in state $|\phi\rangle$ as $|\langle\psi|\phi\rangle|^2$ where $\langle\psi|\phi\rangle : \mathbb{C} \rightarrow \mathbb{C}$ is the inner product of the two state vectors [16].

Axiom 4 (Generalized Born Rule). *The possibility of measuring the state $|\psi\rangle$, having prepared state $|\phi\rangle$, is given by the image of:*

$$\langle\psi|\phi\rangle : \{\bullet\} \rightarrow \{\bullet\} \tag{2}$$

In the relational model, bases are characterized as particular generalizations of groups known as *groupoids* [14,17]. Groupoids can be viewed as groups where multiplication is relaxed to be a partial function.

Definition 7. *For a system H, a* basis *Z is a direct sum (disjoint union) of abelian groups $Z = G_0 \oplus G_1 \oplus ...$ where $|Z| = |H|$. Multiplication with respect to this list of groups will be written as $\bullet_Z$ and is defined in the following way. For elements $x, y \in Z$ such that $x \in G_i$ and $y \in G_j$ we have the partial function:*

$$x \bullet_Z y = \begin{cases} x +_{G_i} y & i = j \\ undefined & otherwise \end{cases} \tag{3}$$

This makes Z an abelian groupoid *with groupoid multiplication $\bullet_Z$.*

We will sometimes take a categorical perspective on groupoids. A groupoid $Z = \bigoplus^N G_i$ made up N groups is a category whose set of objects is isomorphic to the set of groups $\{G_i\}$ and whose morphisms are elements of Z, e.g. $x \in Z$ such that $x \in G_1$ is a morphism $x : G_1 \rightarrow G_1$.

At first guess, one might be motivated by the intuition that a basis for a system breaks it up into parts, and so a basis would be a partition of H. This is not a bad start, however, bases have additional structure: namely that we can copy, delete and combine them at will. This idea is used to motivate Definition 7 by abstracting bases to special dagger-commutative Frobenius algebras (Definition 19) that we call classical structures [7].

Classical structures' properties, allowing the copying, deleting, and combining that accompany classical (as opposed to quantum) information, give them this name. The definition of a special dagger-commutative Frobenius algebra in our model is given in Section 3, and we can interpret it through pair of lemmas corresponding to the traditional model and the relational model of quantum computation.

Lemma 8 ([7]). *The classical structures in the category of finite dimensional Hilbert spaces and linear maps are exactly the orthonormal bases.*

Lemma 9 ([10,17]). *The classical structures in the category of sets and relations are exactly the abelian groupoids.*[2]

---

[2] In [13] this connection is extended to the non-abelian case where it is shown that all relative Frobenius algebras are groupoids.

Z   X

2	2
1	1
0	0
$\mathbb{Z}_3$	$\mathbb{Z}_3$

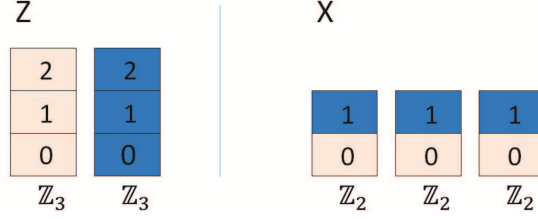|		
1	1	1
0	0	0
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$

Fig. 1. An example of two complementary bases on the system of six elements. Here $Z = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $X = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The two classical states of Z are each three element subsets and are colored in pink and blue. The unbiased states of X to which they correspond are colored to match.

2.1 Complementarity

Complementary bases are important features of quantum theory. In the general setting, complementary bases are understood as mutually unbiased bases in a certain sense [3]. In relations there is a more direct characterization:[3]

Theorem 10 ([10]). *Two bases Z and X are complementary if and only if they are of the following form. Basis $Z = \bigoplus^{|H|} G$ and basis $X = \bigoplus^{|G|} H$ given by copies of abelian groups G and H respectively.*

This theorem follows from the requirement that the classical states of one basis must be isomorphic to the unbiased states of its complement. We will return to this idea in the Section 5 when we address the quantum Fourier transform. Classical and unbiased states of bases in the relational model are specified in the following definitions that instantiate abstract definitions in [3]. An example on the six element system is illustrated with Figure 1.

Definition 11 ([10]). *The* classical states *of a basis $Z = \bigoplus^N G$ are the subsets corresponding to the groups $G_0, G_1, ...$ where we forget the group structure. They will often be denoted $|G_i\rangle$.*

Definition 12 ([10]). *The* unbiased states *for a basis $Z = \bigoplus^N G$ are subsets U such that for a fixed $g \in G$, $|U\rangle = \bigoplus^N \{g\}$. Thus there is exactly one element in each unbiased U from each component G_i of Z.*

Example 13. Take $Z = \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{0_a, 1_a, 0_b, 1_b\}$. The classical states of Z are $|G_a\rangle = |0_a \vee 1_a\rangle$ and $|G_b\rangle = |0_b \vee 1_b\rangle$. The unbiased states of Z are $|U_0\rangle = |0_a \vee 0_b\rangle$ and $|U_1\rangle = |1_a \vee 1_b\rangle$.

It is easy to check that bases as specified by Theorem 10 have the property that each classical state $|G_i\rangle$ of the basis Z corresponds to one unbiased state of X and vice versa. This allows us to call these bases mutually unbiased, i.e. complementary [10].

---

[3] Theorem 10 holds as long as we consider bases to be the same if their lists of groups are isomorphic.

2.2 The Model QCRel

Definition 14. *Axioms 1-4, and subsequent definitions, specify the abstract process theory for* quantum computation in relations: QCRel.

Theorem 15. *QCRel is a model of quantum computation with sets and unitary relations.*

Proof. This is true by construction. The axioms on the preceding section can be interpreted as structures in any dagger compact category. In particular, **FHilb**, the category of finite dimensional Hilbert spaces and linear maps, is a dagger compact category in which interpretation of those axioms results in the usual Hilbert space quantum mechanics [1]. **Rel**, the category of sets and relations, is also dagger compact. It is the interpretation of the abstract axioms for quantum computation in **Rel**, rather than **FHilb**, that produces QCRel as a model. References that covers the dagger compact abstraction and some of its interpretation in different categories are [5,14].

It is worth noting that QCRel can be simply viewed as a local hidden variable theory. We consider the set H to be the set of ontic states such that for $\phi \subseteq H$ the state $|\phi\rangle$ is non-deterministically in any of the ontic states in the subset ϕ. From this perspective, QCRel provides a non-deterministic local hidden variable model for computational aspects of quantum mechanics [2]. This means that protocols exist for entanglement, teleportation, and, as we show in this paper, some familiar blackbox algorithms.
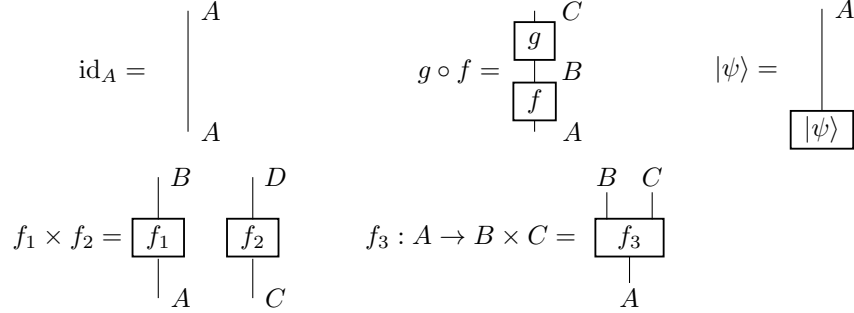
3 Graphical Notation

In this section, we introduce a simple graphical notation that is commonly used in the literature for abstract process theories [4,5]. See [19] for a survey of these diagrams. This notation will ease the inclusion of higher level proofs in our particular setting. In the context of this paper, this graphical notation acts as a more formal circuit-like model to present protocols and algorithms. For systems A and B, we represent the relation $f : A \to B$ as:

$$\boxed{f}\ \substack{B \\ \\ A}$$
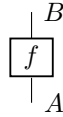
"reading" the diagram from bottom to top. We represent individual systems (the identity morphism on them), sequential composition, states, and composite

systems with the following diagrams, where relations are not necessarily unitary:

$$\mathrm{id}_A = \quad\begin{matrix}A\\ \Big|\\ A\end{matrix} \qquad\qquad g\circ f = \quad\begin{matrix}C\\ \boxed{g}\\ B\\ \boxed{f}\\ A\end{matrix} \qquad\qquad |\psi\rangle = \quad\begin{matrix}A\\ \Big|\\ \boxed{|\psi\rangle}\end{matrix}$$

$$f_1 \times f_2 = \begin{matrix}B & D\\ \boxed{f_1} & \boxed{f_2}\\ A & C\end{matrix} \qquad\qquad f_3 : A \to B \times C = \begin{matrix}B\ \ C\\ \boxed{f_3}\\ A\end{matrix}$$

The state relation is understood where the missing input wire means a map from the "empty" diagram which is the set $\{\bullet\}$, so that all relations $|\psi\rangle : \{\bullet\} \to A$ give subsets of A.[4]

Definition 16. *The* adjoint *of a relation* $f : A \to B$ *is its relational converse* $f^{-1} : B \to A$.

This is what motivated our definition of unitary relations and is graphically represented by simply flipping the diagram upside down.

Having introduced this notation, we are now able to collect some standard results from the literature [3], where they are often defined as more general structures. We include these definitions for use in later proofs, and so present them in terms specific and sufficient for our setting.

Definition 17. *A comonoid is a triple* $(A, \curlyvee, \varphi)$ *of a system* A, *a relation* $\curlyvee : A \to A \times A$ *called the comultiplication, and a relation* $\varphi : A \to \{\bullet\}$ *called the counit, satisfying coassociativity and counitality equations:*

$$\curlyveedownup \quad = \quad \curlyveedownup \qquad\qquad \curlyvee\varphi \quad = \quad \Big| \quad = \quad \varphi\curlyvee \qquad\qquad (4)$$

In equational form, writing $\delta = \curlyvee$ and $\epsilon = \varphi$, these are $(\delta \times \mathrm{id}_A) \circ \delta = (\mathrm{id}_A \times \delta) \circ \delta$ and $\mathrm{id}_A \times \epsilon \circ \delta = \mathrm{id}_A = \epsilon \times \mathrm{id}_A \circ \delta$. Using the relational converse, we can flip the constraining equations upside down to obtain the associated monoid $(A, \delta^{-1} = \curlywedge, \epsilon^{-1} = \delta)$. We can then ask for the comonoid and monoid to interact in various ways.

Definition 18. *A comonoid* $(A, \curlyvee, \varphi)$ *and its monoid under the relational converse form a* dagger-Frobenius algebra *when the following equation holds:*

$$\curlywedgeveeright \quad = \quad \curlyveewedgeleft \qquad\qquad \delta^{-1} \times id_A \circ id_A \times \delta = id_A \times \delta^{-1} \circ \delta \times id_A \qquad (5)$$

---

[4] In any dagger compact category states are morphisms from the monoidal unit, which, in **Rel** is the singleton [1].

Definition 19. *A* classical structure *is a dagger-Frobenius algebra* $(A, \Yleft, \varphi)$ *satisfying the* specialness (6) *and* symmetry (7) *conditions:*

$$\Yleft = \Big| \qquad\qquad \delta^{-1} \circ \delta = id_A \tag{6}$$

$$\Yleft = \bigcup \qquad\qquad \nu \circ \delta \circ \epsilon^{-1} = \delta \circ \epsilon^{-1} \tag{7}$$

where the crossing systems represent the relation that swaps the left and right hand systems, i.e. $\nu := \{((a, b), (b, a)) | a, b \in A\}$. *In general, dagger-Frobenius algebras that obey* (7) *are called* symmetric.

As was noted in Lemma 9 these classical structures exactly correspond to groupoids. The map $\Ygate : A \times A \to A$ corresponds exactly to groupoid multiplication defined by Equation 3. When these classical structures are defined with Hilbert spaces and linear maps instead of sets and relations they exactly correspond to orthonormal bases, as stated in Lemma 8.

Complementary classical structures can also be defined graphically. Here we color the maps for two different classical structures differently.

Definition 20 (Complementarity). *Two classical structures* $(A, \Yleft, \varphi)$ *and* $(A, \Yleft, \varphi)$ *are* complementary *when the following equation holds:*

$$\Yleft = \varphi \tag{8}$$

This was shown to correspond to the usual notion of unbiased bases for classical structures in the category of Hilbert spaces and linear maps in [3].

4   Unitary Oracles

In order to model blackbox quantum algorithms in this setting, we must define the oracles themselves. We do this by building up from an abstract definition of the controlled-not gate in the literature. Let the gray classical structure on a system A be given by a basis $Z = \bigoplus^{|H|} G$ and the white classical structure be a basis $X = \bigoplus^{|G|} H$. The comonoid for the gray dot is then the relation $\Yleft : A \to A \times A$ that for $x, a, b \in H$ is given by

$$\{(x, (a, b)) \mid a \bullet_Z b = x\}.$$

Definition 21 ([22]). *The abstract controlled-not is given by a composition of the comonoid for Z and the monoid for X:*

$$\Ygate \qquad\qquad \begin{array}{l} CNOT\colon H \times H \to H \times H :: \\ \{((x, y), (a, b \circ_X y)) \mid a \bullet_Z b = x\}. \end{array} \tag{9}$$

It can be shown that in the traditional quantum setting of Hilbert spaces and linear maps, this exactly corresponds to the usual controlled-not. This also leads to the following useful theorem, which can be abstractly proved.

Theorem 22 (Complementarity via a unitary [22]). *Two classical structures are complementary if and only if the abstract controlled-not from Definition 21 is unitary.*

This allows us to prove the following about complementary bases in QCRel.

Theorem 23. *Two bases (Z and X) in QCRel are complementary, in the sense of Theorem 10, if and only if the relation in* (9) *is a bijection.*

Proof. The relevant relation can clearly be seen to be the composite in Definition 21 as:

$$\{((a,b,y),(a,b\circ_X y))\}\circ\{((x,y),(a,b,y))\mid a\bullet_Z b=x\}. \tag{10}$$

Thus the abstract proof of Theorem 22 from [22] goes through unchanged.

An oracle is then introduced as a controlled-not where we have embedded a particular kind of relation that abstractly must be a self-conjugate comonoid homomorphism [22]. We construct such relations in the following lemmas.

Definition 24. *Let G and H be groupoids with with groupoid multiplications $\bullet_G$ and $\bullet_H$ respectively. Let $id_G = \bigcup_{X\in Ob(G)} id_X$ and similarly define id_H. A groupoid homomorphism relation $R : G \to H$ obeys the following condition for $g_1, g_2 \in G$:*

$$R(g_1 \bullet_G g_2) = R(g_1) \bullet_H R(g_2) \tag{11}$$

Note that while this in many ways resembles a groupoid homomorphisms, it is actually a weakening of this notion, in that groupoid homomorphism relations are not required to be total functions and have no explicit requirement on their identity morphisms.

Definition 25. *A* monoid homomorphism relation *is a monoid homomorphism in the category of sets and relations. Specifically, let A and B be sets equipped with monoids $(A, \curlywedge, \varphi)$ and $(B, \blacklozenge, \bullet)$ respectively. A relation $r : A \to B$ is a monoid homomorphism when it obeys the following two conditions:*

$$r \circ \curlywedge = \blacktriangle \circ (r \times r) \tag{12}$$

$$r \circ \varphi = \bullet \tag{13}$$

A comonoid homomorphism relation *is defined similarly, using duals of the above conditions.*

Lemma 26. *A groupoid homomorphism relation that is surjective on objects is a monoid homomorphism relation.*

Proof. Included in Appendix A.

We then dualize the proof of Lemma 26 to conclude that:

Lemma 27. *Let $F : H \to G$ be a functor such that F^{op} is a groupoid homomorphism relation that is surjective on objects. F is a comonoid homomorphism relation.*

We call these comonoid homomorphism relations *classical relations*. These are relations that properly preserve the structure of the bases where classical data is embedded. In the quantum case they take basis elements to basis elements. Some examples in QCRel are listed in Appendix B. In order to define unitary oracles, we also need these relations to be self-conjugate:

Definition 28 ([22]). *In a monoidal dagger-category, a comonoid homomorphism $f : (A, \text{\Y}, \bullet) \to (B, \text{\Y}, \text{\Q})$ between dagger-Frobenius comonoids is self-conjugate when the following property holds:*

$$
\begin{array}{ccc}
\includegraphics & = & \boxed{f^\dagger}
\end{array}
\tag{14}
$$

The meaning of this equation in relations is explicated in the following lemma.

Lemma 29. *All classical relations $f : Z^A \to Z^B$ between groupoids $Z^A = \bigoplus^N G^A$ and $Z^B = \bigoplus^{N'} G^B$ are self-conjugate.*

Proof. In QCRel, our dagger-Frobenius structures are groupoids and, if they are complementary to some other groupoid, then they are of the form $Z^A = \bigoplus^N G$ and $Z^B = \bigoplus^{N'} H$. We annotate the definition of self-conjugacy for some arbitrary element (g, n), the element g from the n-th group. Recall from Section 2.2 that $f^\dagger = f^{-1}$ in QCRel.

$$
\begin{array}{ccc}
\includegraphics & = & \boxed{f^{-1}}
\end{array}
\tag{15}
$$

Thus, a relation f is self-conjugate if and only if for all elements (g, n) it is the case that $[f^{-1}(g^{-1}, n)]^{-1} = f^{-1}(g, n)$. From Lemma 27 the converse of the classical relation f is a monoid homomorphism relation whose multiplication is the groupoid operation

Classical relations, as self-conjugate comonoid homomorphisms, lead to unitary oracles.

Definition 30 (Oracle [22]). *Given a groupoid Z^A : $(A, \curlyvee, \bullet)$, a pair of complementary groupoids Z^B : $(B, \curlyvee, \varphi)$ and X^B : $(B, \curlyvee, \varphi)$, and a classical relation R : $(A, \curlyvee, \bullet) \to (B, \curlyvee, \varphi)$, an* oracle *is defined to be the following endomorphism of $A \times B$:*
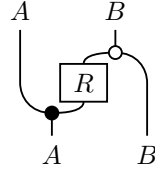
$\mathrm{OracleRel}(R) : A \times B \to A \times B ::$

$\{((x,y),(a, c \circ_X y)) \mid$

$\qquad \exists b \in A, s.t.\ a \bullet_{Z^A} b = x \text{ and } bRc\}.$

Theorem 31. *Oracles are unitary.*

Proof. Proved in the abstract setting for Definition 30 in [22], when R is a self-conjugate comonoid homomorphism. Though there are others, classical relations R are necessary and sufficient in our cases as the algorithms that follow additionally require that the comonoids be part of classical structures.

Corollary 32. *OracleRel is a bijection.*

Proof. This follows directly from Theorem 31 and Corollary 4.

5 The Fourier Transform in Relations

In these algorithms we use the quantum Fourier transform for relations [11]. This is a generalized quantum Fourier transform whose definition is motivated through the relationship between classical and unbiased states of two bases. For abelian groups G and H, consider two groupoids $Z = \bigoplus^{|H|} G$ and $X = \bigoplus^{|G|} H$ to be complementary bases of the same system.

Definition 33. *The* quantum Fourier transform in relations *corresponds to preparing classical states of Z and measuring them against classical states of X.*

Example 34. Take $G = \mathbb{Z}_2 = \{0,1\}$, $H = \mathbb{Z}_1 = \{\star\}$, $Z = G$ and $X = H \oplus H = \{(\star,0),(\star,1)\}$. The computational basis is the family $|H_g\rangle_{g \in G}$ of classical states for X, i.e. $H_0 = \{(\star,0)\}$ and $H_1 = \{(\star,1)\}$. The quantum Fourier basis is a single classical state $G_\star = \{(\star,0),(\star,1)\}$ for Z. In this case all states can be prepared in the computational basis, but measurement in the quantum Fourier basis is trivial.

Example 35. Take $G = \mathbb{Z}_2 = \{0, 1\}$, $H = \mathbb{Z}_2 = \{a, b\}$, $Z = G \oplus G = \{(0, 0), (1, 0), (0, 1), (1, 0)\}$ and $X = H \oplus H = \{(a, a), (b, a), (a, b), (b, b)\}$. The computational basis is the family $|H_g\rangle_{g \in G}$ of classical states for X, i.e. $H_0 = \{(a, a), (b, a)\}$ and $H_1 = \{(a, b), (b, b)\}$. The quantum Fourier basis is the family $|G_h\rangle_{h \in H}$ of classical states for Z, i.e. $G_a = \{(0, 0), (0, 1)\}$ and $G_b = \{(1, 0), (1, 1)\}$.

See [11] to fully motivate this definition of the Fourier transform in QCRel and for its relationship to the usual Hadamard and Fourier transforms for Hilbert spaces and linear maps.
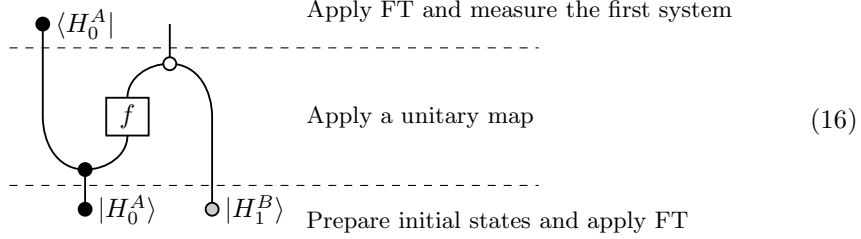
6 The Deutsch-Jozsa Algorithm in QCRel

The well known Deutsch-Jozsa algorithm is an early quantum algorithm that demonstrates a speedup over exact classical computation [8]. It takes as input a function promised to be either constant or balanced and returns which, deterministically using only a single oracle query. In this section, we model the algorithm's steps in QCRel just as it is implemented with Hilbert spaces and linear maps. This approach is somewhat dual to the usual one where different algorithms are compared on the same problem. Here we run the same abstract protocol (implemented in a different model) with the same query complexity and compare the different problems that it solves.

To run this algorithm in QCRel we use two systems. System A has cardinality n and system B has cardinality ≥ 2. Take $Z^A = \bigoplus^{|H^A|} G^A$ and $X^A = \bigoplus^{|G^A|} H^A$ to be complementary bases of A. Take $Z^B = \bigoplus^{|H^B|} G^B$ and $X^B = \bigoplus^{|G^B|} H^B$ to be complementary bases of B, such that X^B has at least two classical states. In analogy with the usual specification, the algorithm proceeds with the following steps.

1. Prepare A in the zero state $|G_0^A\rangle$. Prepare B in the state given by the second classical state of Z^B, i.e. $|G_1^B\rangle$.
2. Apply the Fourier transform, as given by Definition 33, to each system, resulting in states $|H_0^A\rangle$ and $|H_1^B\rangle$ respectively.
3. Apply an oracle (Definition 30), built from a classical relation $f : Z^A \to Z^B$.
4. Again apply the Fourier transform to system A and then measure it in the Z basis.

This sequence of steps is an instance in sets and relations of the abstract Deutsch-Jozsa algorithm from [21], which translates to the following relation where we have already applied the Fourier transform to the input and output systems:

Apply FT and measure the first system

Apply a unitary map $\qquad\qquad$ (16)

Prepare initial states and apply FT

that is explicitly written as:

$$\mathrm{DJAlg}(f) :: \{\bullet\} \times \{\bullet\} \to \{\bullet\} \times B$$
$$= \langle H_0^A| \times \mathrm{id}_B \circ \mathrm{OracleRel}(f) \circ |H_0^A\rangle \times |H_1^B\rangle$$
$$= \{((\bullet, \bullet), (\bullet, z)) \mid z \in H_1^B \text{ and } \exists y \in H_0^A, \text{ s.t. } yfz\}.$$

Theorem 36 ([21]). *In any dagger compact category with complementary bases, the algorithm in Equation 16 will, with a single oracle query, distinguish* constant *and* balanced *classical relations* $f : Z^A \to Z^B$ *according to the following abstract definitions. Here* $|x\rangle$ *is a classical point of* Z^A *and the zero scalar* 0 *is, in* **Rel**, *the empty relation:*

$$
constant: \quad \boxed{f} \;=\; \overset{\displaystyle x}{\bigtriangledown}\!\!\bullet \;=\; |x\rangle \circ \bullet
\qquad\qquad
balanced: \quad \boxed{f} \;=\; 0,
$$

(17)

where $\overset{2}{\circ}$ *is the dagger adjoint of the second classical state of* X^B.

That these definitions coincide with the usual ones for constant and balanced functions is shown in [21]. In QCRel, the effect $\bullet$ is $\langle H_1^A|$, which acts as a measurement of system A after applying the oracle. We illustrate the details of the QCRel model of this algorithm by example and then with general definitions.

Example 37. Take $A = \{0, 1, 2, 3\}$ and $B = \{a, b, c, d\}$ to be four element systems. We define complementary bases on these systems as the following:

System A	System B
$Z^A = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ s.t.	$Z^B = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ s.t.
$G_0^A = \{0, 1\}, G_1^A = \{2, 3\}$	$G_0^B = \{a, b\}, G_1^B = \{c, d\}$
$X^A = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ s.t.	$X^B = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ s.t.
$H_0^A = \{0, 2\}, H_1^A = \{1, 3\}$	$H_0^B = \{a, c\}, H_1^B = \{b, d\}$

From Equation 17, we then define constant and balanced classical relations using the following dictionary:

$$\vcenter{\hbox{\includegraphics{}}} \quad = \{(0, \bullet), (2, \bullet)\}, \quad \text{the adjoint of the first classical state of } X^A \quad (18)$$

$$\vcenter{\hbox{\includegraphics{}}}_x \quad = \{(\bullet, a), (\bullet, b)\} \text{ OR } \{(\bullet, c), (\bullet, d)\}, \quad \text{a classical state of } Z^B \quad (19)$$

$$\vcenter{\hbox{\includegraphics{}}}^2 \quad = \{(b, \bullet), (d, \bullet)\}, \quad \text{adjoint of the second classical state of } X^B \quad (20)$$

$$\vcenter{\hbox{\includegraphics{}}} \quad = \{(\bullet, 0), (\bullet, 2)\}, \quad \text{the first classical state of } X^A \quad (21)$$

Thus there are two constant classical relations[5] $f : Z^A \to Z^B$, one for each classical state of Z^B. They are:

$$\{(0, a), (0, b), (2, a), (2, b)\} \quad \text{and} \quad \{(0, c), (0, d), (2, c), (2, d)\}.$$

By Theorem 36, balanced classical relations are those which do not relate 0 or 2 to either b or d. There are four balanced classical relations for this example:

$$\{(0,c),(2,c),(1,d),(3,d)\} \qquad \{(0,a),(1,b),(2,c),(3,d)\}$$
$$\{(2,a),(3,b),(0,c),(1,d)\} \qquad \{(0,a),(2,a),(1,b),(3,b)\}$$

For a classical relation promised to be in one of these two classes, we can distinguish which with a single oracle query.

We generalize these definitions of constant and balanced classical relations to the following:

Definition 38. *Let* $Z^A = \oplus^N G_i$. *A* constant *relation* $f : Z^A \to Z^B$ *relates all* id_{G_i} *to a single classical state of* Z^B.

Definition 39. *A relation* $f : Z^A \to Z^B$ *is* balanced *when no element in the first classical state of* X^A *is related to an element in the second classical state of* X^B.

Theorem 40. *The Deutsch-Jozsa algorithm defined above distinguishes constant relations from balanced relations in a single oracle query.*

Proof. This follows immediately from the abstract proof of the Deutsch-Jozsa algorithm in [21].

This result shows that we are able to model the Deutsch-Jozsa algorithm in the nondeterministic classical setting of QCRel.

[5] A list of more example classical relations is given in Appendix B.

7 Single-shot Grover's Algorithm

The usual Grover's algorithm [**?**] takes as input a set S and an indicator function $f : S \to \{0, 1\}$ and outputs an element $s \in S$ such that $f(s) = 1$. Though the algorithm is usually probabilistic and runs a repeated series of "Grover steps", here we consider the deterministic version that runs with a single step. In this section we will consider the generalization of the single-shot Grover algorithm where the codomain of the indicator function is allowed to be an arbitrary group [21]. Our setup requires the set S, as one system, as well as another system B. We define the basis $Z^S = \bigoplus^{|H^S|} G^S$ and $X^S = \bigoplus^{|G^S|} H^S$ on the S system. System B has complementary bases $Z^B = \bigoplus^{|H^B|} G^B$ and $X^B = \bigoplus^{|G^B|} H^B$. Let $|\sigma\rangle$ be the first classical state of X^B, e.g. is $X^B = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ then $|\sigma\rangle = \{(\star, 1), (\star, 3)\}$, where 1 and 3 are the non-identity elements of that factors of X^B. Let $\langle \rho |$ be the converse of a classical state of X^S. Recall that $|G_0^S\rangle = \{(\star, g) \,|\, g \in G^S \text{ is the first factor group of } Z^S\}$ is a classical point of Z^S, and that, by the complementary relationship of classical and unbiased points (Section 5), $|H_0^S\rangle \cong \{(\star, \mathrm{id}_{G_i^S}) \,|\, G_i^S \text{ is a factor group of } Z^S\}$.

In QCRel, the algorithm proceeds by the following steps:

1. Prepare system S in the state $|G_0\rangle$ and system B in the state $|\sigma\rangle = |0 \vee 1\rangle$.
2. Apply the Fourier transform to system S, resulting in state $|H_0\rangle$.
3. Apply the oracle for a classical indicator relation $f : Z^S \to Z^B$.
4. Apply a diffusion relation $D : S \to S$ to system S.
5. Measure system S in the X^S basis.

The diagrammatic presentation for this procedure from [21] is:

$$(22)$$
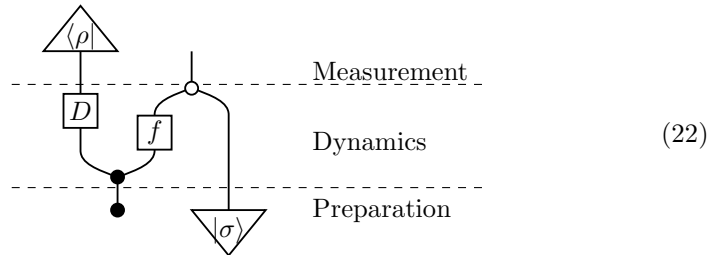
where numerical scalars have been dropped as there is only one non-zero scalar in QCRel. [6] Recall that $\bullet : \{\star\} \to S$ relates the singleton to the elements of H_0 and that ϕ is its relational converse. We will use the map $\bullet \circ \phi : S \to S$ in the following definition. Here there is a special relation $D : S \to S$ called the diffusion operator and defined abstractly in [21]:

---

[6] Recall that scalars in a monoidal category with identity object I are maps $s : I \to I$. Thus in **Rel** $I = \{\star\}$, so the only scalars are the empty relation and the identity relation on the singleton set.

$$
\boxed{D} \;=\; \Big| \;-\; \substack{\bullet \\ \bullet} \qquad\qquad D := \{(x,x)\,|\,x \in S\} \,\triangle\, (H_0 \times H_0) \qquad (23)
$$

where the subtraction of two relations is given by the symmetric difference of their images. Explicitly then, the relational model for Grover's algorithm is:

$$
\mathrm{Grover}(f) : \{\bullet\} \times \{\bullet\} \to \{\bullet\} \times B
$$
$$
= \langle \rho| \times \mathrm{id}_B \circ D \times \mathrm{id}_B \circ \mathrm{OracleRel}(f) \circ |H_0^S\rangle \times |\sigma\rangle
$$
$$
= \{((\bullet,\bullet),(\bullet, c \circ_X x)) \,|
$$
$$
x \in \sigma, y \in \rho, \mathrm{id}_{G_n}, b, z \in S \text{ s.t. } z \bullet_{Z^S} b = \mathrm{id}_{G_n} \text{ and } bfc, zDy\}
$$

Theorem 41. *Equation 22 is zero only for classical states of X^S denoted $|\rho\rangle$ that satisfy the following equation:*

$$
\sigma \circ f \circ \rho = \sigma \circ f \circ |G_0\rangle \qquad (24)
$$

Proof. Proven in [21]. See Section 3.2 equation (34).

Here $|\sigma\rangle$ is, in general, any fixed classical state of X^B. This allows a generalization of the single-shot Grover's algorithm where the cardinality of system B is increased as investigated in [21]. Consequently, the LHS of Equation 24 tests if any element in the classical state $|\rho\rangle$ is related to any of the elements in $|\sigma\rangle$. The RHS tests if any of the elements of G_0 are related to $|\sigma\rangle$.

Proposition 42. *The QCRel single-shot Grover algorithm only returns states $|\rho\rangle$ such that for all $h \in H_0^S$, $s \in \rho$ and $x \in \sigma$*

$$
hfx \;\;=\;\; \neg(sfx).
$$

In other words, the only elements can be possibilistically measured (via the QCRel Born rule in Axiom 4) are elements of S that have the opposite mapping to σ, under the relation f, than elements of H_0^S.

Proof. Theorem 41 gives an abstract proof and this proposition can be seen to instantiate it by the definitions given here.

Example 43. Let $S = \{0,1,2,3\}$ and choose $Z^S = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $X^S = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ as G (black) and H (white) bases respectively, so that $G_0 = \{0,1\}$ and $H_0 = \{0,2\}$. Let B be the four element system with the same bases and choose $|\sigma\rangle = |1 \vee 3\rangle$. The diffusion operator is then given by

$$
D := \{(0,0),(1,1),(2,2),(3,3)\} - \{(0,0),(0,2),(2,0),(2,2)\}
$$
$$
= \{(1,1),(3,3),(0,2),(2,0)\}.
$$

In this case, D happens to be a bijection, it is a unitary relation and thus a possible evolution in QCRel.[7] Let f be the classical relation[8] $\{(0,2),(2,2),(1,3),(3,3)\}$, where elements of H_0^S are not related to elements of $|\sigma\rangle$. Thus the above algorithm will only return classical states of X^S that *are* related, under f, to $|\sigma\rangle$. The only possible outcome state is $|1 \vee 3\rangle$.

Example 44. This is the same as the above example, but take f to be the classical relation $\{(0,0),(2,0),(0,1),(2,1)\}$. As an element of H_0^S is related to $|\sigma\rangle$, the algorithm will return classical states of X^S which are *not* mapped to $|\sigma\rangle$, i.e. the state $|1 \vee 3\rangle$.

8   The Groupoid Homomorphism Promise Algorithm

This section models the group homomorphism algorithm from [22] in QCRel. The quantum version of the algorithm, which operates in **FHilb**, takes as input a blackbox function $f : G \to A$ promised to be one of the homomorphisms between group G and abelian group A. It then outputs the identity of the homomorphism. In that paper the full identification algorithm is built up by multiple calls to an instance of the problem for cyclic groups.[9] It is this cyclic group subroutine that we consider here. In the relational setting we will move from groups to groupoids. Let groupoid H be complementary to groupoid G and groupoid B be complementary to groupoid A. The QCRel GroupHomID algorithm then takes as input a groupoid isomorphism $f : G \to A$. Let $|\rho\rangle$ be a classical states of H, and $|\sigma\rangle$ be a classical state of B.

The algorithm has the following abstract specification [22]:

Measure the left system

Apply a unitary map   (25)

Prepare initial states
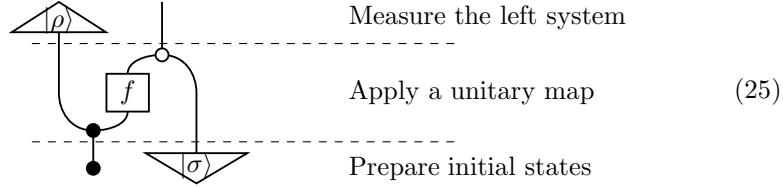
Let the factor groups of a groupoid G be denoted G_n. This gives the following relational model for the algorithm:

$$\text{GroupHomID}(f) : \{\bullet\} \times \{\bullet\} \to \{\bullet\} \times B$$
$$= \langle\rho| \times \text{id}_B \circ \text{OracleRel}(f) \circ |H_0\rangle \times |\sigma\rangle$$
$$= \{((\bullet,\bullet),(\bullet, c \circ_X x)) \mid$$
$$x \in \sigma, y \in \rho, \text{id}_{G_n}, b \in A \text{ s.t. } y \bullet_G b = \text{id}_{G_n} \text{ and } bfc\}$$

---

[7] This will not be the case whenever S has more than two factor groups. Unitarity is a stringent condition on processes in QCRel.

[8] See Appendix B for a list of classical relations $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

[9] Making use of the structure theorem for abelian groups to complete the general case.

Theorem 45. *The algorithm defined by (25) has output state $|\rho\rangle$ only when for some $x \in \rho$ and some $y \in \sigma$ we have $(y, x) \in f$.*

Proof. The verification in [22] simplifies the algorithm in Equation 25 to:

$$
\vcenter{\hbox{}} \quad = \quad \{(\bullet, (\bullet, x)) \mid x f^{-1} y \text{ for some } y \in \rho\}, \qquad (26)
$$

where we see that post-selection on the left hand system implies the theorem's condition.

Theorem 46. *If f is a groupoid isomorphism then the algorithm in Equation 25 returns all states.*

Proof. Groupoid isomorphisms relate every element of the domain to some element in the codomain and relate every element of the codomain to some element of the domain.

Still, we can imagine running the algorithm from (25) where any classical relation f is allowed as input to obtain non-trivial outcomes.

A Appendix: Proof of Lemma 26

Proof. Throughout this proof we refer to a groupoid as a category where the elements of the groupoid are the morphisms. From this perspective a group is a groupoid with a single object. Consider a groupoid homomorphism relation $R : G \to H$ on objects X, A, B of G and morphisms f of G. In order to show that R is a monoid homomorphism relation we first show that it preserves the unit (13). We have $R(\bigcup_{X \in \mathrm{Ob}(G)} \mathrm{id}_X) = \bigcup_{Y \in \mathrm{Ob}(H)} \mathrm{id}_Y$. Recall that for a set A, $R(A) = \bigcup_{a \in A} R(a)$. It is that case that

$$
R(\bigcup_{X \in \mathrm{Ob}(G)} \mathrm{id}_X) = \bigcup_{X \in \mathrm{Ob}(G)} R(\mathrm{id}_X) = \bigcup_{X \in \mathrm{Ob}(G)} \mathrm{id}_{R(X)} \quad \text{def. of group hom. rel.}
$$

$$(27)$$

$$
= \bigcup_{R(X) \in \mathrm{Ob}(G)} \mathrm{id}_{R(X)} = \bigcup_{Y \in \mathrm{Ob}(H)} \mathrm{id}_Y \quad \text{surjective on objects}
$$

$$(28)$$

where we have used the fact that R is surjective on objects, which implies that every object of H is in the image of R and that $|\mathrm{Ob}(G)| \geq |\mathrm{Ob}(H)|$.

The second monoid homomorphism condition (12) is to preserve multiplication, i.e. that for subsets K and J of G we have

$$
R(K +_G J) = R(K) +_H R(J). \qquad (29)
$$

Here we recall that for two sets A and B, $A + B = \{a + b | a \in A \text{ and } b \in B\}$.
Thus,

$$R(K +_G J) = R(\bigcup_{k \in K, j \in J} k +_G j) = \bigcup_{k \in K, j \in J} R(k +_G j) \tag{30}$$

$$= \bigcup_{k \in K, j \in J} R(k) +_H R(j) \qquad \text{def. of group hom. rel.} \tag{31}$$

$$= R(K) +_H R(J). \tag{32}$$

This completes the proof.

B Appendix: Classical Relations

In this appendix we list examples of classical relations as calculated by a Mathematica package available at: `https://github.com/willzeng/GroupoidHomRelations`

Classical relations $\mathbb{Z}_3 \to \mathbb{Z}_3$:

$\{(0,0), (0,1), (0,2)\}$
$\{(0,0),(1,1),(2,2)\}$
$\{(0,0),(1,2),(2,1)\}$

Classical relations $\mathbb{Z}_4 \to \mathbb{Z}_4$:

$\{(0,0),(0,1),(0,2),(0,3)\}$
$\{(0,0),(1,1),(2,2),(3,3)\}$
$\{(0,0),(2,1),(0,2),(2,3)\}$
$\{(0,0),(3,1),(2,2),(1,3)\}$

The classical relations from $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ are:

$\{(0,2),(2,2),(1,3),(3,3)\}$ $\{(0,0),(1,1),(2,2),(3,3)\}$
$\{(0,2),(2,2),(1,3),(2,3)\}$ $\{(0,0),(1,1),(2,2),(2,3)\}$
$\{(0,2),(2,2),(0,3),(3,3)\}$ $\{(0,0),(0,1),(2,2),(3,3)\}$
$\{(0,2),(2,2),(0,3),(2,3)\}$ $\{(0,0),(0,1),(2,2),(2,3)\}$
$\{(2,0),(3,1),(0,2),(1,3)\}$ $\{(0,0),(2,0),(1,1),(3,1)\}$
$\{(2,0),(3,1),(0,2),(0,3)\}$ $\{(0,0),(2,0),(1,1),(2,1)\}$
$\{(2,0),(2,1),(0,2),(1,3)\}$ $\{(0,0),(2,0),(0,1),(3,1)\}$
$\{(2,0),(2,1),(0,2),(0,3)\}$ $\{(0,0),(2,0),(0,1),(2,1)\}$

References

1. Abramsky, S., Coecke, B.: Categorical quantum mechanics. Handbook of quantum logic and quantum structures: quantum logic pp. 261–324 (2008)
2. Abramsky, S., Heunen, C.: Operational theories and categorical quantum mechanics. arXiv preprint arXiv:1206.0921 (2012)
3. Coecke, B., Duncan, R.: Interacting quantum observables: Categorical algebra and diagrammatics. New Journal of Physics 13(4), 043016 (2011)
4. Coecke, B., Kissinger, A.: Picturing Quantum Processes. Cambridge University Press (to appear 2015)
5. Coecke, B., Paquette, É.O.: Categories for the practising physicist. In: New Structures for Physics, pp. 173–286. Springer (2011)
6. Coecke, B., Pavlovic, D.: The Mathematics of Quantum Computation and Technology, chap. Quantum Measurements Without Sums. Taylor and Francis (2006)

7. Coecke, B., Pavlovic, D., Vicary, J.: A new description of orthogonal bases. Mathematical Structures in Computer Science 23, 555–567 (June 2013)

8. Deutsch, D., Jozsa, R.: Rapid solutions of problems by quantum computation. Proceedings of the Royal Society of London A (439), 553–558 (1992)

9. Ellerman, D.: On classical finite probability theory as a quantum probability calculus. arXiv preprint arXiv:1502.01048 (2015)

10. Evans, J., Duncan, R., Lang, A., Panangaden, P.: Classifying all mutually unbiased bases in Rel. arXiv preprint arXiv:0909.4453 (2009)

11. Gogioso, S., Zeng, W.: Fourier transforms from strongly complementary observables. arXiv preprint arXiv:1501.04995 (2015)

12. Hanson, A.J., Ortiz, G., Sabry, A., Tai, Y.T.: Discrete quantum theories. Journal of Physics A: Mathematical and Theoretical 47(11), 115305 (2014)

13. Heunen, C., Contreras, I., Cattaneo, A.S.: Relative Frobenius algebras are groupoids. arXiv preprint arXiv:1112.1284 (2011)

14. Heunen, C., Vicary, J.: Categories for Quantum Theory: An Introduction. Oxford University Press (to appear 2015)

15. James, R.P., Ortiz, G., Sabry, A.: Quantum computing over finite fields. arXiv preprint arXiv:1101.3764 (2011)

16. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge university press (2010)

17. Pavlovic, D.: Quantum and classical structures in nondeterministic computation. In: et. al, P.B. (ed.) Third International symposium on Quantum Interaction, Lecture Notes in Artifical Intelligence, vol. 5494, pp. 143–157. Springer (2009)

18. Schumacher, B., Westmoreland, M.D.: Modal quantum theory. In: Coecke, B., Panangaden, P., Selinger, P. (eds.) QPL 2010, 7th workshop on Quantum Physics and Logic. pp. 145–149 (2010)

19. Selinger, P.: A survey of graphical languages for monoidal categories. Springer Lecture Notes in Physics (813), 289–355 (2011), `arxiv.org/abs/0908.3347`

20. Spekkens, R.: Evidence for the epistemic view of quantum states: A toy theory. Physical Review A 75(032110) (2007)

21. Vicary, J.: Topological structure of quantum algorithms. Proceedings of 28th Annual ACM/IEEE Symposium on Logic in Computer Science pp. 93–102 (2013)

22. Zeng, W., Vicary, J.: Abstract structure of unitary oracles for quantum algorithms. In: Proceedings of the 11th International Workshop on Quantum Physics and Logic. No. 172, EPTCS (2014), `arXiv:1406.1278`