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. In this paper we construct abstract models of blackbox quantum algorithms using a model of quantum computation in sets and relations, a setting that is usually considered as a model for nondeterministic classical computation. This work provides an alternative model of quantum computation (QCRel) that, 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 models 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 [3][4][6][7]. This approach captures all the familiar structure of quantum computation from teleportation to quantum secret-sharing [21] and locates the particular quantum setting of Hilbert spaces as an instance of more general abstract process theories [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 [20][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 model some example quantum algorithms as non-deterministic classical algorithms while preserving their query-complexity (and, in fact, all their abstract structure). The second thrust is for 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 [10][13][18][19], and some even discuss protocols [16], these works have not developed the structures necessary to model quantum algorithms.
The next section of this paper will construct our chosen model of quantum information. This is the setting of sets and relations, rather than Hilbert spaces and linear maps, and it will be introduced by rephrasing the axioms of quantum mechanics. Section 3 will introduce 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.

Acknowledgements The author would especially like to acknowledge the useful discussions and encouragement from Bob Coecke, Chris Heunen, and Jamie Vicary as well as funding support from The Rhodes Trust and AFOSR grant FA9550-14-1-0079.

2 The model of quantum computation in relations

We begin with definitions of the key components of quantum computation in this new setting, e.g. systems, states, bases, observables, etc. The following definitions are motivated by examples from [5] and [12], 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 $\psi \subseteq H$.

Our notation is to write the set label as a ket. Thus $|\psi \lor \phi\rangle$ denotes the state with elements in the union of sets $\psi$ and $\phi$. We often use $|\psi\rangle$ to mean the relation $\{\bullet\} \rightarrow H$ that relates the singleton to all the elements in $\psi$.

Axiom 2. A composite system $H$ of $n$ systems $H_1, ..., H_n$ is given by the Cartesian product of the subsystem sets so that $H = H_1 \times ... \times H_n$. Composite states will be written as $|\psi \otimes \phi\rangle$ and are any subset of the product set $H$.

Definition 1. For 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 $yR^{-1}x$.

Definition 2. 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 $\circ$ is the usual composition of relations.

Corollary 3 ([12]). 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 a state 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 4. 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 if the outcome state \( |\psi\rangle \) is possible. We give an example to illustrate:

**Example 5.** 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 of \( |\psi\rangle \) is possible, or it is the empty relation that we interpret to mean the measurement outcome \( |\psi\rangle \) is impossible. It is clear that the outcome \( |\psi\rangle \) is possible if there exists some element of \( H \) in both \( \psi \) and \( \phi \). 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 to describe measurement in our model.

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

\[
\langle \psi | \phi \rangle : \{\bullet\} \rightarrow \{\bullet\}
\]

(1)

In the relational model, bases are characterized as particular generalizations of groups known as groupoids [15]. Groupoids can be viewed as groups where multiplication is relaxed to be a partial function.

**Definition 6.** For a system \( H \), a basis \( Z \) is list of abelian groups \( Z = G_0 \oplus G_1 \oplus ... \) where \( \sum_{G_i} |G_i| = |H| \). 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:

\[
x \bullet_Z y = \begin{cases} 
i = j & x + G_i \ y \\ otherwise & undefined \end{cases}
\]

(2)

This makes \( Z \) an abelian groupoid with groupoid multiplication \( \bullet_Z \).

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, basis have additional structure: namely that we can copy, delete and combine them at will. This idea is used to motivate Definition 6 by abstracting bases to classical structures.

**Definition 7 ([15]).** Special dagger-commutative Frobenius algebras are classical structures.

Their classical-like properties, allowing copying, deleting, and combining, give them this name. The definition of a special dagger-commutative Frobenius algebra in our model is given in Section 3, but we can interpret it through pair of lemmas corresponding to the traditional-model and the relational-model of quantum computation.

**Lemma 8 ([8]).** Classical structures in the category of finite dimensional Hilbert spaces and linear maps are exactly orthogonal bases.
Fig. 1. An example of two complementary bases on the system of six elements. Here $Z = Z_3 \oplus Z_3$ and $X = Z_2 \oplus Z_2 \oplus Z_2$. The two classical points of $Z$ are each three element subsets and are colored in pink and blue. The unbiased points of $X$ to which they correspond are colored to match.

Lemma 9 ([17]). Classical structures in the category of sets and relations are exactly abelian groupoids.

2.1 Complementarity

Complementary bases in the relational setting are understood using a different abstraction that more narrowly specifies their structure:

Theorem 10 ([15]). 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 points of one observable must be isomorphic to the unbiased points of its complement. We will return to this idea in the Section 5 when we address the quantum Fourier transform.

Classical and unbiased points of bases in the relational model are specified in the following corollaries. An example on the six element system is illustrated with Figure 1.

Corollary 11. The classical points of a basis $Z$ are the subsets of $H$ corresponding to the groups $G_0, G_1, ...$ where we forget the group structure. They will often be denoted $|G_i\rangle$.

Corollary 12. The unbiased points for a basis $Z$ on a system $H$ are subsets $U \subseteq H$ such that for a fixed $g \in G$,

$$|U\rangle = \bigcup_{h \in H} g.$$ 

Thus there is exactly one element in $U$ from each component $G_i$ of $Z$.

1 In [14] this connection is extended to the non-abelian case where it is shown that all relative Frobenius algebras as groupoids.

2 Theorem 10 holds as long as we consider bases to be the same if their lists of groups are isomorphic.
Example 13. Take \( Z = \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{0_a, 1_a, 0_b, 1_b\} \). The classical points of \( Z \) are \( |G_0\rangle = |0_a \lor 1_a\rangle \) and \( |G_1\rangle = |0_b \lor 1_b\rangle \). The unbiased points of \( Z \) are \( |U_0\rangle = |0_a \lor 0_b\rangle \) and \( |U_1\rangle = |1_a \lor 1_b\rangle \).

It is easy to check that complementary observables as specified by Theorem 10 have the property that each classical point \( |G_i\rangle \) of the observable \( Z \) corresponds to one unbiased point of \( X \) and vice versa, i.e. \( |U_i\rangle = |H_i\rangle \).

2.2 Phases

Phases are also defined in this relational setting. In Hilbert space quantum mechanics a quantum phase for an \( n \)-dimensional system is given by the vector
\[
\left( e^{i\phi_1} \right) \begin{pmatrix} \vdots \\ e^{i\phi_n} \end{pmatrix}.
\]
These quantum phases form an abelian group and can be applied as phase gates. Their relational counterparts are described by the following lemma from [15]:

Lemma 14. For a basis \( Z = \bigoplus_i^N G_i \), the phase group \( B(Z) \) is given by \( \prod_i^N G_i \).

Example 15. Consider the basis \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) for the four element system \( \{00, 01, 10, 11\} \). Let \( |\psi\rangle \) be the state \( |00 \lor 10\rangle \). Application of the phase 11 results in
\[
11|00 \lor 10\rangle = |11 \lor 01\rangle.
\]

We are also able to interpret GHZ states and density matrices in sets and relations.

Definition 16. For a basis \( Z \), a GHZ state is given by
\[
\text{GHZ}_Z := \{ (a, b, c) \mid \forall a, b, c \in Z, a \bullet Z b \bullet Z c = id_G, \text{ for some } i \}.
\]

Definition 17. For a state \( |\psi\rangle \), the density matrix \( |\psi\rangle \langle \psi| \) is given by the relation \( xRy \) s.t. \( x, y \in \psi \).

2.3 The model QCRel

Definition 18. Axioms 1-4, and subsequent definitions, specify the abstract process theory for quantum computation in relations: QCRel.

Theorem 19. 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, \( \mathbf{FHilb} \), 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.

\( \mathbf{Rel} \), the category of sets and relations, is also dagger compact. It is the interpretation of the abstract axioms for quantum computation in \( \mathbf{Rel} \), rather than \( \mathbf{FHilb} \), that produces QCRel as a model. A reference that covers the dagger compact abstraction and some of its interpretation in different categories is [15].
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 $\phi$. From this perspective, QCRel provides a non-deterministic local hidden variable model for computational aspects of quantum mechanics. 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 to discuss abstract process theories. 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

```
    B
   /
  f
 /
A
```

“reading” the diagram from bottom to top. We represent individual systems (the identity morphism on them), sequential composition, composite systems, and states with the following diagrams:

```
    A
  id_A =
    A

    C
  g \circ f =
    B
   /
  f
 /
A

    B
   /
  f\times g =
    A
   /
  g
 /
A

    C
  f : A \to B \times C =
    B
   /
  f
 /
A
```

The state relation is understood by defining the “empty” diagram as the set $\{\bullet\}$, so that all relations $|\psi\rangle : \{\bullet\} \to A$ give subsets of $A$.

**Definition 20.** The adjoint of a relation $f : A \to B$ is its relational converse $f^{-1} : B \to A$.

---

3 See [1] for details of this interpretation as an operational theory.
4 In any dagger compact category states are morphisms from the monoidal unit, which, in Rel is the singleton.
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 \[4\], 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 21.** A comonoid is a triple \((A, \gamma', \phi)\) of a system \(A\), a relation \(\gamma' : A \to A \otimes A\) called the comultiplication, and a relation \(\phi : A \to \{0, 1\}\) called the counit, satisfying coassociativity and counitality equations:

\[
\begin{align*}
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array} & = \\
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array}
\end{align*}
\]

Using the relational converse, we can flip the constraining equations upside down to obtain the associated monoid. We can then ask for the comonoid and monoid to interact in various ways.

**Definition 22.** A comonoid \((A, \gamma', \phi)\) is dagger-Frobenius when the following equation holds:

\[
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array} = \\
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array}
\]

**Definition 23.** A classical structure is a commutative dagger-Frobenius comonoid \((A, \gamma', \phi)\) satisfying the specialness condition:

\[
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array} = \\
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array}
\]

**Definition 24.** A dagger-Frobenius comonoid is symmetric when the following condition holds:

\[
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array} = \\
\begin{array}{c}
\text{\begin{tikzpicture}[baseline=-.5ex]
\node (a) at (0,0) {A};
\node (b) at (1,0) {A};
\node (c) at (2,0) {A};
\end{tikzpicture}}
\end{array}
\]

where the crossing systems represent the relation that swaps the left and right hand systems. As was noted in Lemma \[8\] these classical structures exactly correspond to groupoids. The map \(\cdot : A \times A \to A\) corresponds exactly to groupoid multiplication defined by Equation \[2\] When these classical structures are defined with Hilbert spaces and linear maps instead of sets and relations they exactly correspond to bases, as stated in Lemma \[8\].

Our definition for complementary bases is also motivated from an abstract construction\[2\]. Here we color the maps for two different classical structures differently.
Definition 25 (Complementarity). Two special symmetric dagger-Frobenius comonoids \((A, \mathcal{V}, \varphi)\) and \((A, \mathcal{V}', \varphi')\) are complementary when the following equation holds:

\[
\begin{array}{c}
\text{Diagram}
\end{array}
\]

(7)

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 from 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 \(\mathcal{V} : A \to A \times A\) that for \(x, a, b \in H\) given by

\[
\{(x, (a, b)) \mid a \cdot_Z b = x\}.
\]

Definition 26 ([22]). The abstract controlled-not is given by a composition of the comonoid for \(Z\) and the monoid for \(X\):

\[
\begin{array}{c}
\text{Diagram}
\end{array}
\]

whose explicit relation is:

\[
\text{CNOT} : H \times H \to H \times H : \{(x, y), (a, b \circ_X y) \mid a \cdot_Z b = x\}. 
\]

(8)

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 27 (Complementarity via a unitary [22]). Two symmetric dagger-Frobenius algebras are complementary if and only if the abstract controlled-not from Definition 26 is unitary.

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

Theorem 28. Two bases in QCRel are complementary, in the sense of Theorem 10, if and only if the relation in Equation 8 is a bijection.

Proof. The relevant relation can clearly be seen to be the composite in Definition 26 as

\[
\{(a, b, y), (a, b \circ_X y) \} \circ \{(x, y), (a, b, y) \} \mid a \cdot_Z b = x\}. 
\]

(9)

Thus the abstract proof of Theorem 27 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 29.** Given groupoids \(G\) and \(H\) and groupoid homomorphism \(F : G \to H\), we can define an associated groupoid homomorphism relation \(R : G \to H\) where, for morphism \(x\) in \(G\) and morphism \(y\) in \(H\),

\[ xRy \iff F(x) = y. \]

**Lemma 30.** Given a groupoid homomorphism that is surjective on objects, its associated groupoid homomorphism relation \(R : G \to H\), is a monoid homomorphism relation.

**Proof.** A groupoid homomorphism \(F : G \to H\) is a functor that, for objects \(X, A, B\) of \(G\) and morphisms \(f\) of \(G\), takes

\[ X \mapsto F(X) \]

\[ (f : A \to B) \mapsto (F(f) : F(A) \to F(B)) \]

such that

\[ F(g \circ_G f) = F(g) \circ_H F(f) \]

\[ F(id_X) = id_{F(X)}. \]

We now show that the groupoid homomorphism relation \(R\) associated to \(F\) is a monoid homomorphism relation.

First, we must show that it preserves the unit, i.e. that for \(X \in \text{Ob}(G)\) and \(Y \in \text{Ob}(H)\) we have

\[ R(\bigcup_X id_X) = \bigcup_Y id_Y. \]

Recall that for a set \(A\) with elements \(a\), \(R(A) = \bigcup R(a)\). It is that case that

\[ R(\bigcup_X id_X) = \bigcup_X R(id_X) \tag{10} \]

\[ = \bigcup_X id_{R(X)} \quad \text{def. of functor} \tag{11} \]

\[ = \bigcup_{R(X)} id_{R(X)} \tag{12} \]

\[ = \bigcup_Y id_Y \quad \text{surjective on objects} \tag{13} \]

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

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

\[ R(K +_G J) = R(K) +_H R(J). \tag{14} \]

Here we recall that for two sets \(A\) and \(B\), \(A + B = \bigcup (a + b)\) for all \(a \in A\) and \(b \in B\). Thus,

\[ R(K +_G J) = R(\bigcup_{k,j} k +_G j) = \bigcup_{k,j} R(k +_G j) \tag{15} \]

\[ = \bigcup_{k,j} R(k) +_H R(j) \quad \text{def. of functor} \tag{16} \]

\[ = R(K) +_H R(J). \tag{17} \]
This completes the proof.

**Note 31.** In fact, when the monoid is part of a classical structure (and so given by groupoid multiplication) it is easy to see that all the monoid homomorphism relations come in the form of Lemma 30.

We then dualize the proof of Lemma 30 to conclude that:

**Lemma 32.** For a functor $F : H \to G$ such that $F^\ast$ is a groupoid homomorphism that is surjective on objects, $F$ defines 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 A. In order to define unitary oracles, we will also need these relations to be self-conjugate:

**Definition 33.** In a monoidal dagger-category, a comonoid homomorphism $f : (A, \mathcal{G}, \phi) \to (B, \mathcal{H}, \psi)$ between dagger-Frobenius comonoids is self-conjugate when the following property holds:

$$f = f^\dagger$$

**Lemma 34.** All classical relations $f : Z^A \to Z^B$ between groupoids $Z^A = \bigoplus N G^B$ 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:

$$f^{-1}(g, n) = f^{-1}(g^{-1}, n) \cdot [f^{-1}(g^{-1}, n)]^{-1}$$

---

5 These examples were generated with Mathematica code that is available at https://github.com/willzeng/GroupoidHomRelations
Thus, a relation 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 32 the inverse of the classical relation \(f\) is a groupoid homomorphism, so this condition will hold.

Classical relations, as self-conjugate comonoid homomorphisms, will allow us to define unitary oracles.

**Definition 35 (Oracle [22])**. Given a groupoid \(Z^A : (A, \triangleright, \triangleright)\), a pair of complementary groupoids \(Z^B : (B, \triangleright, \triangleright)\) and \(X^B : (B, \triangleright, \triangleright)\), and a classical relation \(R : (A, \triangleright, \triangleright) \to (B, \triangleright, \triangleright)\), an oracle is defined to be the following endomorphism of \(A \times B\):

\[
\text{OracleRel} : A \times B \to A \times B :: \{(x, y), (a, c \circ_X y) \mid \exists b \in A, s.t. a \bullet_Y b = x \text{ and } bRc\},
\]

In our setting this morphism is exactly

\[
\text{OracleRel} : A \times B \to A \times B :: \{(x, y), (a, c \circ_X y) \mid \exists b \in A, s.t. a \bullet_Y b = x \text{ and } bRc\},
\]

and we are able to recall the following theorem:

**Theorem 36**. Oracles are unitary.

**Proof**. Proved in the abstract setting for Definition 35 in [22]. In that proof, oracles are shown to be unitary when \(f\) is a self-conjugate comonoid homomorphism. Any classical relation, by Lemma 32, will be a self-conjugate comonoid homomorphism. Though there are others, classical relations will be sufficient for our purposes as the algorithms that follow have the additional requirement that the comonoids be part of classical structures, in which case classical relations are the only ones.

**Corollary 37**. \(\text{OracleRel}\) is a bijection.

**Proof**. This follows directly from Theorem 36 and Corollary 3.

## 5 The Fourier transform in relations

In these algorithms we use the relational quantum Fourier transform for relations [11]. This is a generalized quantum Fourier transform whose definition is motivated as a relationship between classical and unbiased points of two observables. 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 38**. The quantum Fourier transform in relations corresponds to preparing classical points of \(Z\) and measuring them against classical points of \(X\).
Example 39. Take $G = \mathbb{Z}_2 = \{0, 1\}$, $H = \mathbb{Z}_1 = \{\ast\}$, $Z = G = \{0, 1\}$ and $X = H \oplus H = \{\ast_0, \ast_1\}$. The computational basis is the family $|H_g \rangle_G$ of classical points for $X$, i.e. $H_0 = \{(\ast, 0)\}$ and $H_1 = \{(\ast, 1)\}$. The quantum Fourier basis is a single classical point $G_\ast = \{(\ast, 0), (\ast, 1)\}$ for $Z$. In this case all states can be prepared in the computational basis, but the measurement in the quantum Fourier basis will be trivial.

Example 40. Take $G = \mathbb{Z}_2 = \{0, 1\}$, $H = \mathbb{Z}_2 = \{a, b\}$, $Z = G \oplus G = \{0_a, 1_a, 0_b, 1_b\}$ and $X = H \oplus H = \{a_0, b_0, a_1, b_1\}$. The computational basis is the family $|H_g \rangle_{G_G}$ of classical points for $X$, i.e. $H_0 = \{(a, 0), (b, 0)\}$ and $H_1 = \{(a, 1), (b, 1)\}$. The quantum Fourier basis is the family $|G_h \rangle_{H_H}$ of classical points for $Z$, i.e. $G_a = \{(a, 0), (a, 1)\}$ and $G_b = \{(b, 0), (b, 1)\}$.

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[9]. It takes as input a function promised to be either constant or balanced and returns which deterministically and with a single oracle query. In this section, we model the algorithms 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 $\geq 2$. 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 points. In analogy with the usual specification, the algorithm proceeds with the following steps.

1. Prepare $A$ in the zero state $|G^A_0\rangle$. Prepare $B$ in the state given by second classical point of $Z^B$, i.e. $|G^B_1\rangle$.
2. Apply the Fourier transform, as given by Definition [38] to each system, resulting in states $|H^A_0\rangle$ and $|H^B_1\rangle$ respectively.
3. Apply an oracle from Equation [20] built from a classical relation $f : Z^A \rightarrow Z^B$.
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 [20], which translates to the relation:

![Diagram](image)

Measure the first system

Apply a unitary map

Prepare initial states

\[ f \]

\[ |H^A_0\rangle \]
Theorem 41 ([20]). In any dagger compact category with complementary observables, the algorithm in Equation 22 will, with a single oracle query, distinguish constant and balanced classical relations \( f : Z^A \to Z^B \) according to the following abstract definitions:

\[
\text{constant: } \begin{array}{c}
\bullet \\
\downarrow \\
\circ
\end{array}
\quad f = \downarrow
\quad \text{balanced: } \begin{array}{c}
\bullet \\
\downarrow \\
\circ
\end{array}
\quad f = 0,
\]

where \( \circ \) is the dagger adjoint of the second classical point of \( X^B \).

That these definitions coincide with the usual ones for constant and balanced functions is shown in [20]. In QCRel, the effect \( \circ \) is \( \langle H^B \rangle \), which acts as a measurement of system \( A \) after applying the oracle.

We illustrate the details of the QCRel model of the Deutsch-Jozsa algorithm first by example and then with general definitions.

Example 42. Take \( A = \{0, 1, 2, 3\} \) and \( B = \{a, b, c, d\} \) to be four element systems. We define complementary observables on these systems as the following:

| System A | System B |
|----------|----------|
| \( Z^A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) s.t. \( G^A_0 = \{0, 1\}, G^A_1 = \{2, 3\} \) | \( Z^B = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) s.t. \( G^B_0 = \{a, b\}, G^B_1 = \{c, d\} \) |
| \( X^A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) s.t. \( H^A_0 = \{0, 2\}, H^A_1 = \{1, 3\} \) | \( X^B = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \) s.t. \( H^B_0 = \{a, c\}, H^B_1 = \{b, d\} \) |

From Equation 23 we then define constant and balanced classical relations using the following dictionary:

\[ \circ = \{(0, \bullet), (2, \bullet)\}, \quad \text{the adjoint of the first classical point of } X^A \]  
(24)

\[ \downarrow = \{(\bullet, a), (\bullet, b)\} \text{ OR } \{(\bullet, c), (\bullet, d)\}, \quad \text{a classical point of } Z^B \]  
(25)

\[ \circ \circ = \{(b, \bullet), (d, \bullet)\}, \quad \text{the adjoint of the second classical point of } X^B \]  
(26)

\[ \downarrow = \{(\bullet, 0), (\bullet, 2)\}, \quad \text{the first classical point of } X^A \]  
(27)

Thus there are two constant classical relations \( \circ f : Z^A \to Z^B \), one for each classical point of \( Z^B \). They are:

\[ \{(0, a)(0, b)(2, a)(2, b)\} \quad \text{and} \quad \{(0, c)(0, d)(2, c)(2, d)\} \]  
(28)

\[ A \text{ full list of classical relations is given in the Appendix.} \]
By Definition 41, balanced classical relations are those which do not relate 0 or 2 to either \( b \) or \( d \).

Here is the list of balanced classical relations for this example:

\[
\{(0, c)(2, c)(1, d)(3, d)\}
\[
\{(2, a)(3, b)(0, c)(1, d)\}
\[
\{(0, a)(1, b)(2, c)(3, d)\}
\[
\{(0, a)(2, a)(1, b)(3, b)\}
\]

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 43.** A constant relation \( f : Z^A \rightarrow Z^B \) relates all elements of \( A \) to a single classical point of \( Z^B \).

**Definition 44.** A relation \( f : Z^A \rightarrow Z^B \) is balanced when no element in the first classical point of \( X^A \) is related to an element in the second classical point of \( X^B \).

**Theorem 45.** 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 [20].

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

### 7 Single-shot Grover’s algorithm

Grover’s algorithm[12] takes as input a set \( S \) and an indicator function \( f : S \rightarrow \{0, 1\} \). 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. Our setup requires the set \( S \), as one system, as well as another system \( B = \{0, 1\} \). We define the basis \( Z^S = \bigoplus^N G \) and \( X^S = \bigoplus^{|G|} H \) on the \( S \) system. System \( B \) has complementary bases \( Z^B = Z_2 \) and \( X^B = Z_1 \oplus Z_1 \).

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 \( |\sigma\rangle = |0 \lor 1\rangle \).
2. Apply the Fourier transform to system \( S \), resulting in state \( |H_0\rangle \).
3. Apply the oracle for a classical indicator relation \( R : Z^S \rightarrow Z^B \).
4. Apply a diffusion relation \( D : S \rightarrow S \) to system \( S \).
5. Measure system \( S \) in the \( X^S \) basis.

The diagrammatic presentation for this procedure from [20] is:
where numerical scalars have been dropped as there is only one non-zero scalar in QCRel.

Here there is a special relation \( D : S \to S \) called the diffusion operator and defined abstractly in [20]:

\[
\begin{array}{ccc}
S & & S \\
\downarrow \mathcal{D} & & \downarrow \\
S & & S
\end{array}
\]

(30)

where the subtraction of two relations is given by the symmetric difference of their images.

**Theorem 46** ([20]). Equation 29 is zero only for classical points of \( X^S \) denoted |\( \rho \rangle \) that satisfy the following equation:

\[
\begin{array}{ccc}
\sigma & & \sigma \\
\downarrow R & & \downarrow \\
|\rho \rangle & & |\rho \rangle
\end{array}
\]

(31)

Here |\( \sigma \rangle \) is, in general, any fixed classical point of \( X^B \). This allows a generalization of the single-shot Grover’s algorithm where the cardinality of system \( B \) is increased from 2 as investigated in [20]. Consequently, the LHS of Equation 31 tests if any element in the classical point |\( \rho \rangle \) 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 47.** The QCRel single-shot Grover algorithm only returns states |\( \rho \rangle \) such that for all \( h \in H_0 \), \( s \in \rho \) and \( x \in \sigma \)

\[
gRx = ! (sRx).
\]

In other words, we only see elements of \( S \) that have the opposite mapping to \( \sigma \), under the relation \( R \), than elements of \( H_0 \).

**Proof.** By Theorem 46 and definitions.

**Example 48.** Let \( S = \{0, 1, 2, 3\} \) and choose \( Z^S = Z_2 \oplus Z_2 \) and \( X^S = Z_2 \oplus Z_2 \) 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 \( \sigma = |1 \oplus 3 \rangle \) and \( \rho = |1 \oplus 3 \rangle \). The diffusion operator is then given by

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

As \( D \) is a bijection, it is a unitary relation and thus a possible evolution in QCRel. Take Let \( f \) be the classical relation \( \{(0, 2), (2, 2), (1, 3), (3, 3)\} \). This means that elements of \( H_0 \) are not related to elements of \( |\sigma \rangle \). Thus the above algorithm will only return classical points of \( X^S \) that are mapped to \( |\sigma \rangle \). The only possible outcome state is |\( 1 \oplus 3 \rangle \).

**Example 49.** This will be the same as the above example, but now take \( R \) to be the classical relation \( \{(0, 0), (2, 0), (0, 1), (2, 1)\} \). An element of \( H_0 \) is related to \( |\sigma \rangle \), the algorithm will return classical points of \( X^S \) which are \( not \) mapped to \( |\sigma \rangle \), i.e. the state |\( 1 \oplus 3 \rangle \).

---

7 See Appendix A for a list of classical relations \( Z_2 \oplus Z_2 \to Z_2 \oplus Z_2 \).
8 The groupoid homomorphism promise algorithm

This section models the group homomorphism algorithm from [22] in QCRel. The quantum version of the algorithm 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. It is this cyclic group subroutine that we consider here. In the relational setting, the analogous GroupHomID algorithm takes as input a groupoid isomorphism \( f : G \to A \), where groupoid \( H \) is complementary to \( G \) and groupoid \( B \) is complementary to \( A \). The requirement of oracle unitarity restricts our input from groupoid homomorphisms to groupoid isomorphisms.

**Corollary 50.** Groupoid homomorphisms \( f : G \to A \) are classical relations if and only if they are groupoid isomorphisms.

**Proof.** From Lemma 32, the converse of a classical relation must be a groupoid homomorphism \( f^{-1} : A \to G \).

The algorithm has the following abstract specification [22]:

![Diagram of the algorithm](image)

where \( |\rho\rangle \) and \( |\sigma\rangle \) are classical points of \( H \) and \( B \) respectively. We will denote them as sets by their corresponding groups \( H_\rho \) and \( B_\sigma \).

**Theorem 51.** The algorithm defined by (32) has output state \( |\sigma\rangle \) only when for some \( x \in H_\rho \) and some \( y \in B_\sigma \) we have \( (y, x) \in f \).

**Proof.** The verification in [22] shows that the algorithm in Equation 32 simplifies to:

![Simplified diagram](image)

where \( f^{-1} \) is the relational converse of \( f \) in our setting, and we see that post-selection on the left hand system implies the theorem’s condition.

**Theorem 52.** If \( f \) is a groupoid isomorphism then the algorithm in Equation 32 returns all states.

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

Still, we can imagine running the algorithm from Equation 32 where any classical relation is allowed as input to obtain non-trivial outcomes.

\[ ^8 \text{Making use of the structure theorem for abelian groups to complete the general case.} \]
A Classical Relations

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

**Example 53.** The classical relations from $\mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ are:

\[
\{(0, 0), (1, 0), (2, 0)\} \\
\{(0, 0), (1, 1), (2, 2)\} \\
\{(0, 0), (1, 2), (2, 1)\} \\
\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\}
\]

**Example 54.** The classical relations from $\mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ are:

\[
\{(0, 0), (1, 0), (2, 0), (3, 0)\} \\
\{(0, 0), (1, 1), (2, 2), (3, 3)\} \\
\{(0, 0), (1, 2), (2, 0), (3, 2)\} \\
\{(0, 0), (1, 3), (2, 2), (3, 1)\} \\
\{(0, 0), (0, 2), (1, 0), (1, 2), (2, 0), (2, 2), (3, 0), (3, 2)\} \\
\{(0, 0), (0, 2), (1, 1), (1, 3), (2, 0), (2, 2), (3, 1), (3, 3)\} \\
\{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 1), (2, 2), (2, 3), (3, 0), (3, 1), (3, 2), (3, 3)\}
\]

**Example 55.** The classical relations from $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ are:

\[
\{(0, 2), (2, 2), (1, 3), (3, 3)\} \\
\{(0, 2), (2, 2), (1, 3), (2, 3)\} \\
\{(0, 2), (2, 2), (0, 3), (3, 3)\} \\
\{(0, 2), (2, 2), (0, 3), (2, 3)\} \\
\{(2, 0), (3, 1), (0, 2), (1, 3)\} \\
\{(2, 0), (3, 1), (0, 2), (0, 3)\} \\
\{(2, 0), (2, 1), (0, 2), (1, 3)\} \\
\{(2, 0), (2, 1), (0, 2), (0, 3)\} \\
\{(0, 0), (1, 1), (2, 2), (3, 3)\} \\
\{(0, 0), (1, 1), (2, 2), (2, 3)\} \\
\{(0, 0), (0, 1), (2, 2), (3, 3)\} \\
\{(0, 0), (0, 1), (2, 2), (2, 3)\} \\
\{(0, 0), (2, 0), (1, 1), (3, 1)\} \\
\{(0, 0), (2, 0), (1, 1), (2, 1)\} \\
\{(0, 0), (2, 0), (0, 1), (3, 1)\} \\
\{(0, 0), (2, 0), (0, 1), (2, 1)\}
\]

\[
\{(0, 0), (2, 0), (0, 1), (2, 1)\}
\]
Bibliography

[1] Abramsky, S., Heunen, C.: Operational theories and categorical quantum mechanics. arXiv preprint arXiv:1206.0921 (2012)
[2] Coecke, B., Duncan, R.: Interacting Quantum Observables: Categorical Algebra and Diagrammatics. ArXiv e-prints (Jun 2009)
[3] Coecke, B., Abramsky, S.: Handbook of Quantum Logic and Quantum Structures vol II, chap. Categorical Quantum Mechanics. Elsevier (2008)
[4] Coecke, B., Duncan, R.: Interacting quantum observables: Categorical algebra and diagrammatics. New Journal of Physics 13 (2011)
[5] Coecke, B., Kissinger, A.: Picturing Quantum Processes. Cambridge University Press (to appear 2015)
[6] Coecke, B., Paquette, E.O., Pavlovic, D.: Classical and quantum structuralism. In: Gay, S., Mackie, I. (eds.) Semantic Techniques in Quantum Computation, pp. 29–69. Cambridge University Press (2010)
[7] Coecke, B., Pavlovic, D.: The Mathematics of Quantum Computation and Technology, chap. Quantum Measurements Without Sums. Taylor and Francis (2006)
[8] Coecke, B., Pavlovic, D., Vicary, J.: A new description of orthogonal bases. Mathematical Structures in Computer Science 23, 555–567 (June 2013), http://arxiv.org/abs/0810.0812
[9] Deutsch, D., Jozsa, R.: Rapid solutions of problems by quantum computation. Proceedings of the Royal Society of London A (439), 553–558 (1992)
[10] Ellerman, D.: On classical finite probability theory as a quantum probability calculus (2015), http://arxiv.org/abs/1502.01043
[11] Gogioso, S., Zeng, W.: Fourier transforms from strongly complementary observables (2015), http://arxiv.org/abs/1501.04995
[12] Grover, L.: A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing pp. 212–219 (1996)
[13] Hanson, A.J., Ortiz, G., Sabry, A., Tai, Y.T.: Discrete quantum theories (http://arxiv.org/abs/1305.3292), [pre-print]
[14] Heunen, C., Contreras, I., Cattaneo, A.S.: Relative frobenius algebras are groupoids. arXiv preprint arXiv:1112.1284 (2011)
[15] Heunen, C., Vicary, J.: Categories for Quantum Theory: An Introduction. Oxford University Press (to appear 2015)
[16] James, R.P., Ortiz, G., Sabry, A.: Quantum computing over finite fields, http://arxiv.org/abs/1101.3764
[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 Artificial 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] Spekkens, R.: Evidence for the epistemic view of quantum states: A toy theory. Physical Review A 75(032110) (2007)
[20] Vicary, J.: Topological structure of quantum algorithms. Proceedings of 28th Annual ACM/IEEE Symposium on Logic in Computer Science pp. 93–102 (2013), http://arxiv.org/abs/1209.3917

[21] Zamdzhiev, V.: An Abstract Approach towards Quantum Secret Sharing. Master’s thesis, Department of Computer Science, University of Oxford (2012), http://www.cs.ox.ac.uk/people/bob.coecke/VladimirZamdzhievThesis.pdf

[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 (2014), arXiv:1406.1278