Quantum Speedup and Categorical Distributivity

Peter Hines

University of York
peter.hines@york.ac.uk

Abstract. This paper studies one of the best-known quantum algorithms — Shor's factorisation algorithm — via categorical distributivity. A key aim of the paper is to provide a minimal set of categorical requirements for key parts of the algorithm, in order to establish the most general setting in which the required operations may be performed efficiently.

We demonstrate that Laplaza's theory of coherence for distributivity [13,14] provides a purely categorical proof of the operational equivalence of two quantum circuits, with the notable property that one is exponentially more efficient than the other. This equivalence also exists in a wide range of categories.

When applied to the category of finite-dimensional Hilbert spaces, we recover the usual efficient implementation of the quantum oracles at the heart of both Shor's algorithm and quantum period-finding generally; however, it is also applicable in a much wider range of settings.

Keywords: Category Theory, Quantum Computing, Shor's Algorithm, Monoidal Tensors, Distributivity, Coherence.

This work is dedicated to Samson Abramsky, on the occasion of a birthday with prime factors 2, 3, and 5.

1 Introduction

1.1 Shor's Algorithm: Oracles and Quantum Fourier Transforms

The structure of Shor's algorithm is deceptively simple: an oracle which acts classically on the computational basis computes modular exponentials; this oracle is conjugated by the circuit for the quantum Fourier transform. Up to some relatively simple classical post-processing (computing continued fraction expansions), this is enough to find the prime factors of a number in an exponentially fast time – at least, as compared with the *best known* classical algorithm.

The traditional view of Shor's algorithm and other quantum period-finding algorithms is that their power arises from the quantum Fourier transform; [17] lists Shor's algorithm in the section "Applications of the Fourier transform". This was challenged in [3], where it was demonstrated that the quantum Fourier

B. Coecke, L. Ong, and P. Panangaden (Eds.): Abramsky Festschrift, LNCS 7860, pp. 122–138, 2013.

transform has a *low bubble width* circuit — and any quantum algorithm that is built entirely from low bubble-width circuits has an efficient classical simulation. Thus, it appears that the obstacle to an efficient classical simulation of Shor's algorithm is the oracle for modular exponentiation, rather than the conjugating quantum Fourier transform.

The conclusions drawn in [3] (the claim that the quantum power of Shor's algorithm arises from the central oracle) were, and remain, controversial. However, further evidence to support this claim was provided in [21], where it was demonstrated that modular exponentiation, in of itself, is sufficient. From [21]: *Any classical algorithm that can efficiently simulate the circuit implementing modular exponentiation for general product input states and product state measurements on the output, allows for an efficient simulation of the entire Shor algorithm on a classical computer.* A special case of this, as noted in [21], would be any tensor contraction scheme for the modular exponentiation circuit.

1.2 The Aims of this Paper

This paper describes the circuit for modular exponentiation used in [19] in purely categorical terms. The motivation is to find the most general structures in which this precise form of the oracle may be implemented. We therefore avoid, where possible, categorical machinery that is closely or uniquely associated with the theory of finite-dimensional Hilbert spaces.[1] Instead, we will simply require a category with two monoidal tensors related by a notion of distributivity. As this is established for abstract categories, any concrete category satisfying this simple requirement is sufficient.

1.3 The Structure of the Paper

This paper is divided into two sections: pure category theory, and concrete realisations of this abstract theory.

1. We first use the abstract theory of categories with two monoidal tensors related by distributivity to define endofunctors and further categorical operations on such categories. We use these to define an 'iterator' operation $!^N(\ )$ on endomorphism monoids of such categories, and use Laplaza's theory of coherence for distributivity to give an exponentially efficient factorisation of this operation.
2. The second half of the paper gives a concrete realisation of this operation, and its efficient factorisation, within the quantum circuit paradigm. The $!^N(\ )$ operation has a concrete realisation as the oracle required for quantum period-finding, and its efficient factorisation is exactly Shor's implementation of modular exponentiation oracle.

[1] In particular, the constructions we will present are significantly simpler in the presence of compact closure and biproducts – two categorical properties closely associated with quantum mechanics. However, neither of these categorical properties are necessary, so we work in the more general setting.

2 Basic Definitions

Our abstract setting is that of categories with distributivity, defined in [13,14]:

Definition 1. *A* **category with distributivity** *is a category $\mathcal{C}$ with two distinct symmetric monoidal tensors: the* **multiplicative tensor** $(\otimes) : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ *and the* **additive tensor** $(\oplus) : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ *that are related by natural distributivity monomorphisms*

$$dl_{ABC} : A \otimes (B \oplus C) \to (A \otimes B) \oplus (A \otimes C) \tag{1}$$
$$dr_{XYZ} : (X \oplus Y) \otimes Z \to (X \otimes Z) \oplus (Y \otimes Z) \tag{2}$$

satisfying coherence conditions laid out in [13,14].

The required coherence conditions are decidedly non-trivial and form an infinite family of diagrams that are required to commute, although these may be significantly simplified (from [13], *"we are reduced to a finite number of types of diagrams if we drop unnecessary commutativity conditions"*).

Notation 1. *We adopt the convention of using the Greek alphabet for the structural isomorphisms related to the multiplicative tensor, and the Roman alphabet for the additive tensor. We denote the multiplicative associativity and symmetry isomorphisms by $\tau_{XYZ} : X \otimes (Y \otimes Z) \to (X \otimes Y) \otimes Z$ and $\sigma_{X,Y} : X \otimes Y \to Y \otimes X$, and the additive associativity and symmetry by $t_{XYZ} : X \oplus (Y \oplus Z) \to (X \oplus Y) \oplus Z$ and $s_{XY} : X \oplus Y \to Y \oplus X$. We will frequently appeal to MacLane's coherence theorem for associativity, and treat both the multiplicative and additive tensors as strict.*

We will also denote the multiplicative unit object by I, and the additive unit object by 0.

A special case that is often considered (e.g. [6,7]) is where the distributivity monomorphisms are in fact isomorphisms.

Definition 2. *Let $(\mathcal{C}, \otimes, \oplus)$ be a category with distributivity. We say that is is* **strongly distributive** *when the natural distributivity monomorphisms have global inverses,*

$$dl^{-1}_{ABC} : (A \otimes B) \oplus (A \otimes C) \to A \otimes (B \oplus C) \tag{3}$$
$$dr^{-1}_{XYZ} : (X \otimes Z) \oplus (Y \otimes Z) \to (X \oplus Y) \otimes Z \tag{4}$$

Strongly distributive categories are a special case of Definition 1, so we may still appeal to Laplaza's coherence theorems. Appropriate care will be taken when using commutative diagrams containing inverses of these canonical isomorphisms to ensure that an equivalent result may be derived without the use of inverses. See the proof of Lemma 1 for an example of this.

2.1 Distinguished Objects, and Copying Functors

Strongly distributive categories have two distinguished objects: the additive and multiplicative unit objects $0, I \in Ob(\mathcal{C})$. Their interaction with the two monoidal tensors is given (up to straightforward canonical isomorphism) by the following tables:

$\otimes$	0	I
0	0	0
I	0	I

$\oplus$	0	I
0	0	I
I	I	$I \oplus I$

Observe that $I \oplus I$ is neither 0 nor I; thus in the absence of any further identities, strongly distributive categories have additional distinguished objects.

Definition 3. *We define $2 \in Ob(\mathcal{C})$ to be the additive tensor of two multiplicative units, so $2 = (I \oplus I)$.*

Such objects are considered in [7], where – in the special case that $\otimes$ and $\oplus$ are a product and coproduct respectively – they generate Boolean algebras. The classical logical interpretation is well-established. As noted in [5] the form of distributivity introduced in [13] is entirely unsuitable for linear logic, since distributivity implies a form of 'copying' operation that we now describe:

Lemma 1. *Let $(\mathcal{C}, \otimes, \oplus)$ be a strongly distributive category. Then*

1. *$2 \otimes X \cong X \oplus X$*
2. *for all $f \in \mathcal{C}(X, Y)$, the following diagram commutes:*

$$\begin{array}{ccc} 2 \otimes X & \xrightarrow{1_2 \otimes f} & 2 \otimes Y \\ {\scriptstyle dr^{-1}_{I,I,X}}\uparrow & & \downarrow{\scriptstyle dr_{I,I,Y}} \\ X \oplus X & \xrightarrow{f \oplus f} & Y \oplus Y \end{array}$$

Proof.

1. By distributivity, and the fact that I is the unit object for the multiplicative tensor, $2 \otimes A = (I \oplus I) \otimes A \cong (I \otimes A) \oplus (I \otimes A) \cong A \oplus A$.
2. By naturality, the following diagram commutes:

$$\begin{array}{ccc} (I \oplus I) \otimes X & \xrightarrow{1_{I \oplus I} \otimes f} & (I \oplus I) \otimes Y \\ \downarrow{\scriptstyle dr_{I,I,X}} & & \downarrow{\scriptstyle dr_{I,I,Y}} \\ X \oplus X & \xrightarrow[f \oplus f]{} & Y \oplus Y \end{array}$$

As $(\mathcal{C}, \otimes, \oplus)$ is strongly distributive, we may replace dr_{IIX} in the above diagram by dr^{-1}_{IIX}, and reverse the corresponding arrow:

$$\begin{array}{ccc} (I \oplus I) \otimes X & \xrightarrow{1_{I\oplus I} \otimes f} & (I \oplus I) \otimes Y \\ \uparrow{\scriptstyle dr^{-1}_{I,I,X}} & & \downarrow{\scriptstyle dr_{I,I,Y}} \\ X \oplus X & \xrightarrow[f \oplus f]{} & Y \oplus Y \end{array}$$

□

Definition 4. *Let $(\mathcal{C}, \otimes, \oplus)$ be strongly distributive. We define the* **copying endofunctor** *to be $\delta = (2 \otimes \_) : \mathcal{C} \to \mathcal{C}$.*

This terminology is motivated by the following result:

Proposition 1. *Let $\Delta : \mathcal{C} \to \mathcal{C} \times \mathcal{C}$ be the diagonal functor given by*

- **(Objects)** $\Delta(A) = (A, A)$.
- **(Arrows)** $\Delta(f) = (f, f)$

Then there exists a natural isomorphism (i.e. a natural transformation whose components are isomorphisms) from the composite functor $(\_ \oplus \_)\Delta : \mathcal{C} \to \mathcal{C}$ to the functor $(2 \otimes \_) : \mathcal{C} \to \mathcal{C}$.

We draw this diagrammatically, as follows:

$$\begin{array}{ccccc} & & \mathcal{C} \times \mathcal{C} & & \\ & {\scriptstyle \Delta}\nearrow & \Downarrow & \searrow{\scriptstyle (\_\oplus\_)} & \\ \mathcal{C} & & \xrightarrow[(2\otimes\_)]{} & & \mathcal{C} \end{array}$$

Proof. For arbitrary $X \in Ob(\mathcal{C})$, the components of this natural transformation are given by the distributivity isomorphisms $dl_{I,I,X} : 2 \otimes X \to X \oplus X$ (treating units arrows as strict). The required identity then follows from Lemma 1. □

Remark 1. At first sight, this 'copying' behaviour appears to be at odds with the 'no-cloning' and 'no-deleting' theorems [20,18] of quantum information. However, these are based on tensor products ('multiplicative' tensors), whereas the functor of Definition 4 acts as a form of copying for the additive structure – it is related to the fanout operation [10] rather than the forbidden quantum cloning.

Iterating a copying operation gives a form of exponential growth, as we demonstrate:

Corollary 1. *For all $f \in \mathcal{C}(X, Y)$ and $n \geq 1 \in \mathbb{N}$, there exists canonical isomorphisms $\lambda^{(n)}_X : 2^{\otimes n} \otimes X \to \bigoplus_{j=0}^{2^n-1} X$ making the following diagram commute:*

$$\begin{array}{ccc} 2^{\otimes n} \otimes X & \xrightarrow{\delta^n(f)} & 2^{\otimes n} \otimes Y \\ \downarrow{\scriptstyle \lambda_X} & & \uparrow{\scriptstyle \lambda^{-1}_Y} \\ \bigoplus_{j=0}^{2^n-1} X & \xrightarrow[\oplus_{n=0}^{2^n-1} f]{} & \bigoplus_{j=0}^{2^n-1} Y \end{array}$$

Proof. We give the canonical isomorphisms $\lambda_X^{(n)} : 2^{\otimes n} \otimes X \to \bigoplus_{j=0}^{2^n-1} X$ by induction: we take $\lambda_X^{(1)} = dr_{I,I,X} : 2 \otimes X \to X \oplus X$, and

$$\lambda_X^{(n)} = dr_{I,I,\oplus_{j=0}^{2^{n-1}-1} X} \left(1_2 \otimes \lambda_X^{(n-1)}\right).$$

The above diagram then commutes by naturality. □

We now demonstrate that $\delta : \mathcal{C} \to \mathcal{C}$ is a (weak) *monoidal* endofunctor, for the additive, but not multiplicative, structure.

Proposition 2. *The functor $\delta = (2 \otimes \_) : \mathcal{C} \to \mathcal{C}$ does not preserve the multiplicative monoidal structure, even up to isomorphism; however the additive structure is preserved up to a simple distributivity isomorphism.*

Proof. To see that δ does not preserve the multiplicative tensor, observe that note that

$$\delta(A) \otimes \delta(B) \;=\; (1_2 \otimes \sigma_{A,2} \otimes 1_B)\delta^2(A \otimes B)$$

Thus, unless $\delta(X) \cong \delta^2(X)$ for all $X \in Ob(\mathcal{C})$, the copying functor does not preserve the multiplicative tensor, even up to isomorphism.

However, $\delta(0) \cong 0$, and the following diagram also commutes:

$$\begin{array}{ccc} \delta(A \oplus B) & \xrightarrow{\quad\cong\quad} & \delta(A) \oplus \delta(B) \\ = \big| & & \big| = \\ 2 \otimes (A \oplus B) & \xrightarrow[dl_{(I\oplus I),A,B}]{} & 2 \otimes A \oplus 2 \otimes B \end{array}$$

Since the required isomorphisms are canonical coherence isomorphisms in both cases, $\delta : (\mathcal{C}, \oplus) \to (\mathcal{C}, \oplus)$ is a (weak) monoidal functor. □

2.2 Copying and the Iterator

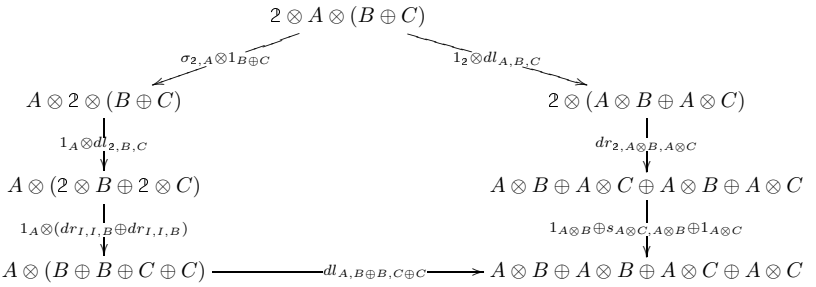
We now study an operation on endomorphism monoids closely related to the copying functor $\delta : (\mathcal{C}, \oplus) \to (\mathcal{C}, \oplus)$.

Definition 5. *Let $(\mathcal{C}, \otimes, \oplus)$ be a strongly distributive category. For all $f \in \mathcal{C}(A, A)$, we define the* $\mathbf{N^{th}}$ **iterator of** *f to be*

$$!^N(f) \;=\; \bigoplus_{j=0}^{N-1} f^j \;\in\; \mathcal{C}\left(A^{\oplus N}, A^{\oplus N}\right)$$

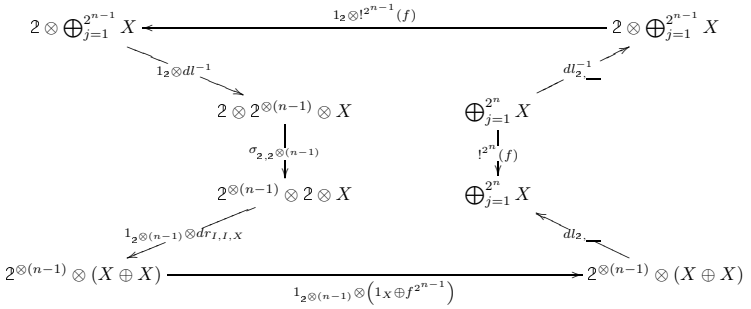
We will give an efficient factorisation of $!^{2^n}(f)$. This will rely on the following interaction of the functor $\delta = (2 \otimes \_) : \mathcal{C} \to \mathcal{C}$, and the multiplicative and additive symmetries $\sigma_{X,Y} : X \otimes Y \to Y \otimes X$ and $s_{A,B} : A \oplus B \to B \oplus A$.

Lemma 2. *Let A, B, C be objects of a strongly distributive category $(\mathcal{C}, \otimes, \oplus)$. Then the following diagram commutes:*



Proof. The commutativity of this diagram follows immediately from the coherence theorems of [13,14] (note that we have elided associativity isomorphisms, for clarity). □

Theorem 2. *For arbitrary $n \geq 1$ and $f \in \mathcal{C}(X, X)$, the arrow $!^{2^{n+1}}(f)$ can be defined in terms of $!^{2^n}(f)$, the functor $(2 \otimes \_)$, and canonical isomorphisms, with the exact relationship expressed by the commutativity of the following diagram:*



Proof. Consider the left hand path in the coherent diagram of Lemma 2 above, from $2 \otimes A \otimes (B \oplus C)$ to $A \otimes B \oplus A \otimes B \oplus A \otimes C \oplus A \otimes C$, along with arrows $f \in \mathcal{C}(B, Y)$ and $g \in \mathcal{C}(C, Z)$. Then naturality of canonical coherence isomorphisms implies the commutativity of the diagram in Figure 1. The required result is then the special case where $X = Y$ and $A = 2^{\otimes n}$. □

2.3 String Diagrams for Categories with Distributivity

Results such as Theorem 2 above may be given as string diagrams, using the conventions formalised in [11,12]. When we have two distinct monoidal tensors,

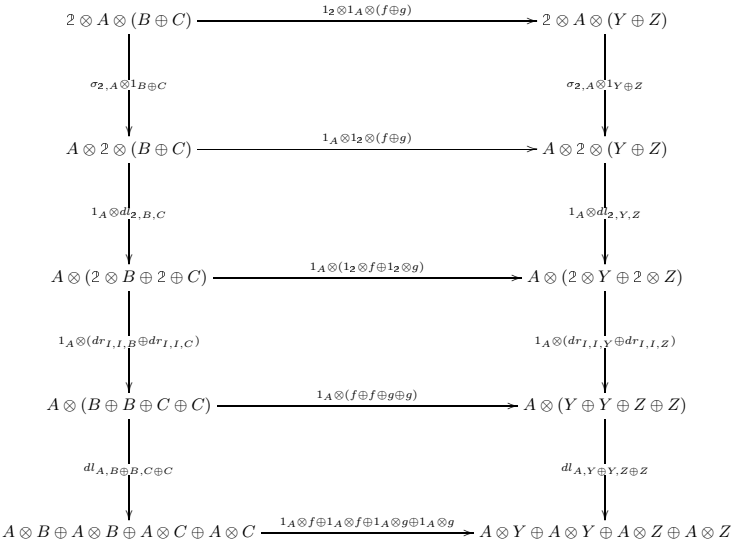


Fig. 1. A technical result implied by naturality

we adopt various conventions to ensure that such a diagrammatic reasoning is still valid:

1. Lines are separated by an implicit *multiplicative* rather than an *additive* monoidal tensor.
2. Operations involving *additive* monoidal tensors are enclosed in a double box.
3. Entering / leaving a double box requires an (implicit) distributivity isomorphism / its inverse. Provided care is taken with labelling of objects, the required canonical isomorphism may be deduced from the type of the operation.

We may then use diagrammatic manipulations on either the diagram as a whole (treating each additive box as a single operation), or on the contents of an individual double box (treating it as an entire diagram in of itself). These conventions ensure that the diagrammatic manipulations of [11,12] are valid, simply by restricting the permitted manipulations.

Using the above, an illustration of Theorem 2 is given in Figure 2.

Corollary 2. *There exists an efficient construction of* $!^{2^n}(f)$ *in* $O(n)$ *steps, based on canonical coherence isomorphisms.*

Proof. This follows by iterating the construction of Theorem 2. A diagrammatic illustration is given in Figure 3. □

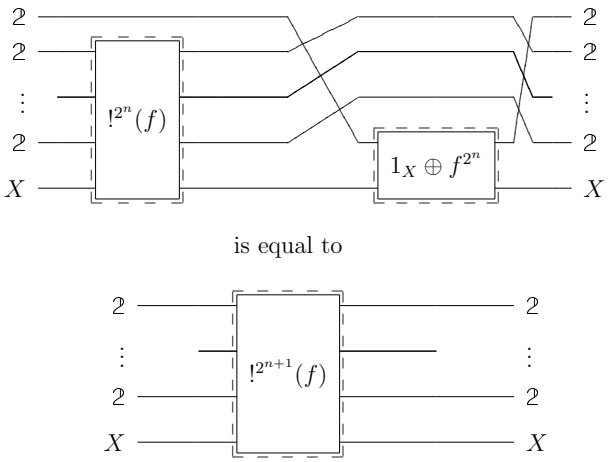


Fig. 2. A 'string diagram' illustration of Theorem 2

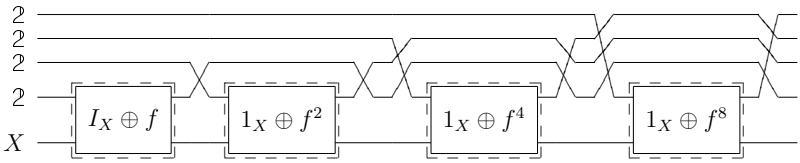


Fig. 3. The efficient construction of $!^{16}(f) = 1_X \oplus f \oplus \ldots \oplus f^{15} \oplus f^{16}$

Table 1. Translating abstract theory into a concrete setting

Abstract category $\mathcal{C}$	**Concrete category** $\mathbf{Hilb_{FD}}$
Multiplicative tensor $H = H_1 \otimes H_2$	**Tensor product** *(Treating two systems as a single compound system).*
Additive tensor $(U \oplus 1)$ $(1 \oplus V)$	**Direct sum** *(U controlled on* $\|0\rangle$*)* *(V controlled on* $\|1\rangle$*)*
Multiplicative unit I	**Complex plane** $\mathbb{C}$
Additive unit 0	**Zero-dim. space** $\{0\}$
Distinguished object $2 = I \oplus I$	**Qubit space** $\mathcal{Q}$, with orthonormal basis $\{\|0\rangle, \|1\rangle\}$

3 Concrete Realisation in Hilbert Space

The following sections assume a small degree of familiarity with quantum circuits and Hilbert spaces. More details may be found in in [17] or any other text on quantum computing and information.

We now consider the constructions of the previous section in the concrete setting of finite-dimensional complex Hilbert spaces. The two monoidal tensors are the familiar tensor product and direct sum — the distributivity isomorphisms relating the these are well-established.

The translation of the basic concepts is given in Table 1. A subtlety of this is the interpretation of the distinguished object 2. The direct sum of two 1-dimensional spaces is of course a two-dimensional space. However, since $\mathcal{Q}$ is built up in this way, we should think of it as having a fixed orthonormal basis specified by the canonical inclusions[2] – this will allow us to use matrix representations for arrows in this category.

Remark 2. A key point of this paper is that the structures required for the central oracle of Shor's algorithm are *not* dependent on the machinery of either traditional quantum mechanics (such as a matrix calculus, or notions of linearity and convergence), or categorical reinterpretations (compact closure, biproduct structures, &c.). However, the existence of matrix representations certainly makes the concrete instantiation simpler, as the following sections will demonstrate.

3.1 Interpreting the Direct Sum in the Circuit Model

In the translation from an abstract to a concrete setting provided in Table 1, the interpretation of the tensor, the multiplicative unit, and the distinguished object 2 are standard. Furthermore, as we are forced by the category theory to specify an orthonormal basis for the two-dimensional qubit space, we are now, for all practical purposes, working within the quantum circuit paradigm. The final connection arises from the interpretation of the direct sum in terms of 'quantum conditionals', or 'controlled operations' [9].

Definition 6. *Let U, V be unitary operations on a finite-dimensional Hilbert space H. The* **controlled operations** *$Ctrl_0U$ and $Ctrl_1V$ are the operations on $\mathcal{Q} \otimes H$ defined by:*

$$Ctrl_0U\,|0\rangle\,|\psi\rangle = |0\rangle\,U\,|\psi\rangle \text{ and } Ctrl_0U\,|1\rangle\,|\psi\rangle = |1\rangle\,|\psi\rangle$$

$$Ctrl_1V\,|0\rangle\,|\psi\rangle = |0\rangle\,|\psi\rangle \quad \text{and } Ctrl_1V\,|1\rangle\,|\psi\rangle = |1\rangle\,V\,|\psi\rangle$$

with standard circuit representations shown in figure 4.

[2] This is, of course, related to the 'classical structures' of [8] — these are a special form of Frobenius algebra that play the role of orthonormal bases in categorical quantum mechanics. They are based on a 'copying' operation; the connection between these, and the $2 \otimes \_$ copying functor of Definition 4, is straightforward.

Denoting the n-qubit identity operation by I_n, these operations have matrix representations given by $C_0U = \begin{pmatrix} U & \mathbf{0} \\ \mathbf{0} & I_n \end{pmatrix}$ and $C_1V = \begin{pmatrix} I_n & \mathbf{0} \\ \mathbf{0} & V \end{pmatrix}$. The direct sum $U \oplus V$ is then simply the composite $U \oplus V = Ctrl_0U.Ctrl_1V = Ctrl_1V.Ctrl_0U$.

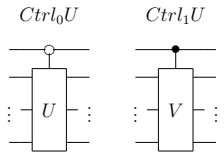


Fig. 4. Quantum circuits for 'Control on 0' and 'Control on 1'

Controlled operations can themselves be controlled. Given 2^n unitary maps $\{U_a\}_{a=0}^{2^n-1}$, the construction of $\bigoplus_{a=0}^{2^n-1} U_a$ is immediate via an n-qubit ancilla. This is illustrated in Figure 5 for the direct sum of 2^3 unitaries, and the 'binary counting' pattern on controls is immediate.

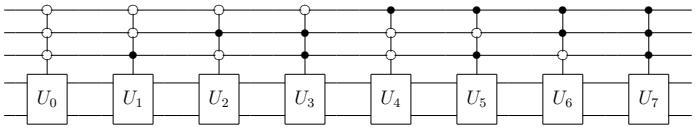


Fig. 5. A circuit for the direct sum $\bigoplus_{a=0}^{7} U_a$

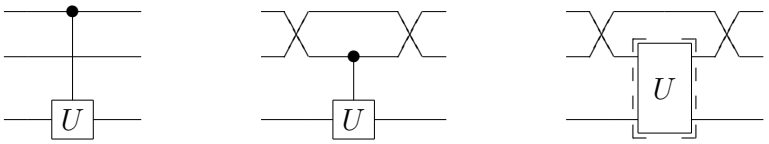


Fig. 6. Three equivalent diagrams

3.2 Controlled Operations and Categorical Swap Maps

In the standard quantum circuit formalism, controlled operations are not necessarily controlled by the qubit directly above them (i.e. the more significant qubit). We treat this as simply a diagrammatic convention, so a circuit where

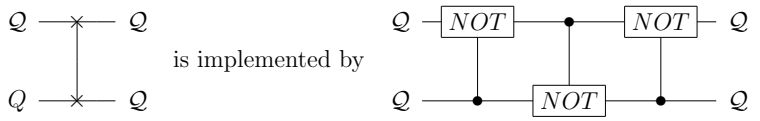


Fig. 7. The multiplicative symmetry via controlled additive symmetries

the control qubit is not adjacent to the controlled operation is implemented using multiplicative symmetries (i.e. qubit swap maps) in the obvious way. Thus, the three circuits of Figure 6 are equivalent, with the first being the usual quantum circuit notation, and the third conforming to the categorical conventions of Section 2.3.

The qubit swap map (i.e. multiplicative symmetry) itself has an interesting categorical interpretation via the standard decomposition shown in Figure 7. The single qubit NOT gate ($NOT\,|0\rangle = |1\rangle$, $NOT\,|1\rangle = |0\rangle$) is the additive symmetry $s_{\mathbb{C},\mathbb{C}}$ of two multiplicative unit objects. Figure 7 expresses an abstract categorical identity relating the multiplicative symmetry $\sigma_{2,2}$, the additive symmetry $s_{I,I}$, and distributivity. Details are left as an interesting exercise.

3.3 Interpreting the Iterator in the Quantum Circuit Paradigm

The interpretation of $!^{2^n}(U) = 1_H \oplus U \oplus U^2 \oplus \ldots \oplus U^{2^n-1}$ for some some unitary operation $U : H \to H$ is immediate; it is simply the sequence of multiply-controlled operations shown in Figure 8. The operational interpretation is immediate:

Proposition 3. *Given an arbitrary quantum state $|\psi\rangle \in H$ and a computational basis ancilla state $|a\rangle$, the circuit of Figure 8 acts on their tensor product as $|a\rangle\,|\psi\rangle \quad \mapsto \quad |a\rangle\,U^a\,|\psi\rangle$.*

Proof. This follows by definition of the action of controlled operations in the quantum circuit model. □

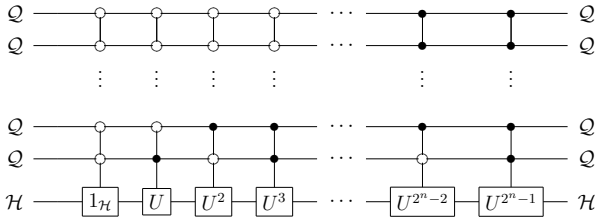


Fig. 8. A circuit for $!^{2^n}(U)$

3.4 Applications of the $!^N(U)$ Operation in Quantum Programming

Quantum circuits acting as $|a\rangle\,|\psi\rangle \;\mapsto\; |a\rangle\,U^a\,|\psi\rangle$ have an important role to play in quantum period-finding algorithms (although, of course, the precise circuit of Figure 9 is *not* used). The best-known period-finding algorithm is, of course, Shor's factorisation algorithm, based on period-finding for modular exponential functions.

Period-finding algorithms rely on a central oracle that acts classically on some subset of the computational basis (we refer to [17] for a formal definition, and [9] for a categorical interpretation in terms of Barr's l_2 functor [4]). Given a classical reversible function f, they require a unitary that acts as $|a\rangle\,|x\rangle \;\mapsto\; |a\rangle\,|f^a(x)\rangle$. Given an oracle U_f for the classical computation f, we may instead write this as $|a\rangle\,|x\rangle \;\mapsto\; |a\rangle\,U_f^a\,|x\rangle$ and observe that the required oracle for quantum period-finding is in fact $!^N(U_f)$, for some suitably large integer $N = 2^n$.

The complete quantum period-finding algorithm (up to some straightforward classical pre- and post- processing) is then simply given by conjugating such an oracle by a quantum Fourier transform, applied to the first register only. For example, in Shor's algorithm the central oracle is required to implement modular exponentials, via the action $|x\rangle\,|1\rangle \;\mapsto\; |x\rangle\,|r^x \;(mod\; K)\rangle$ and hence, by linearity,

$$\left(\sum_{x=0}^{N} |x\rangle\right)|1\rangle \;\mapsto\; \sum_{x=0}^{N} |x\rangle\,|r^x \;(mod\; K)\rangle$$

Given a (readily constructed) quantum oracle U that acts on the computational basis as $U\,|p\rangle \;=\; |rp \;(mod\; K)\rangle$, then, by Proposition 3, the required oracle for Shor's algorithm is $!^N(U)$. Thus the (quantum part of) Shor's algorithm is as shown in Figure 9.

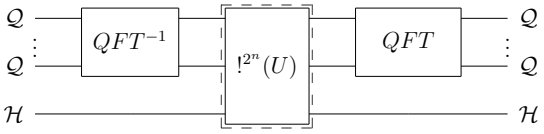


Fig. 9. The quantum circuit in Shor's algorithm

4 An Efficient Circuit for the $!^N(U)$ Operation

The utility of the $!^N(U)$ operation in any period-finding algorithm must rely on an efficient implementation. Implementing the the central oracle using the circuit of Figure 8 would be pointless, given the complexity of constructing such a circuit. Instead, quantum algorithms (in particular, Shor's algorithm) use an exponentially more efficient circuit; we demonstrate that this is exactly the implementation given by Corollary 2.

Proposition 4. *The circuits A and B shown in Figure 10 are equivalent.*

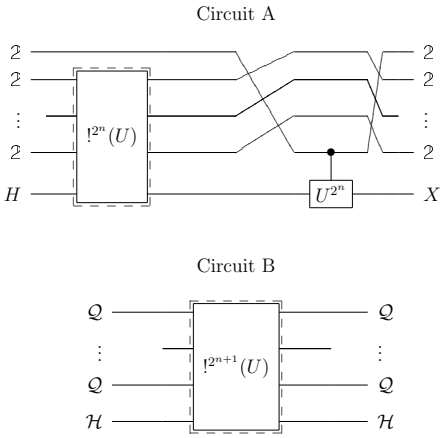


Fig. 10. Two equivalent quantum circuits

Proof. This follows directly from the Theorem 2 – in particular, the diagrammatic illustration given in Figure 2 makes it immediate. Note that the canonical multiplicative symmetry for qubits is drawn as a category-theoretic symmetry, rather than the traditional quantum circuit equivalent shown in Figure 7. □

A simple corollary of Proposition 4 above, and the notational simplifications of Section 3.2, is that we may give a quantum circuit for $!^{2^n}(U)$ using $O(n)$ controlled quantum logic gates as follows:

Corollary 3. *The circuit of Figure 11 implements the* $!^{2^n}(U)$ *operation.*

Proof. This follows by induction on Proposition 4 above. □

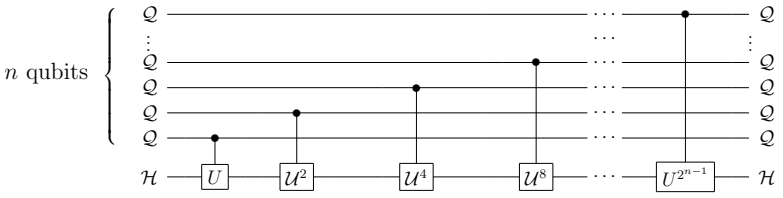


Fig. 11. An efficient implementation of $!^{2^n}(U)$

Remark 3. The efficient circuit of Figure 11 is exactly the circuit used by P. Shor to implement modular exponentiation [19]. From a purely quantum circuit point of view, it is straightforward to demonstrate the equivalence of the circuits of Figure 8 and Figure 11. The interest, from our point of view, is that this equivalence of circuits is an expression of a canonical coherence identity, and thus holds in any strongly distributive category.

4.1 Oracles and Black Boxes

In referring to the circuit of Figure 11 as requiring $O(n)$ primitive gates to implement $!^{2^n}(U)$, we have explicitly *not* considered the complexity of implementing $U, U^2, U^3, \ldots$. Rather, we have treated each of these operations as a 'black box'. For concrete algorithms, this is a serious omission; in particular, any practical realisation of Shor's algorithm also requires some efficient way of implementing (controlled versions of) U^{2^k}, where the operation $U\,|p\rangle \;=\; |rp\ (mod\ K)\rangle$ is as described in Section 3.4.

Fortunately, such an efficient implementation also exists — an oracle for the squaring operation $c \mapsto c^2\ (mod\ K)$ (up to some suitable ancilla, and garbage collection) provides a simple, efficient way of implementing U^{2^k}, for $k = 1, \ldots, n$. This is described in detail in [19]. Note that this technique is not available for arbitrary functions; rather, modular exponentiation is one of the few arithmetic functions for which such an efficient decomposition exists.

5 Conclusions and Future Directions

We have demonstrated that the structural isomorphisms for strongly distributive categories have a role to play in understanding quantum algorithms – or at least that perhaps familiar operations in quantum circuits can be given an abstract interpretation in terms of categorical coherence.

Classically, equivalence up to canonical isomorphism is often used in program transformation, and it is pleasing, although not entirely unexpected, to see it in the quantum setting as well. Of more interest is how little of the machinery of categorical quantum mechanics we have used in establishing these transformations — the only assumption required is that of two monoidal tensors related by distributivity up to isomorphism, and thus the constructions of this paper are valid in a wide range of different categorical and algebraic settings.

Acknowledgements and Apologies

Acknowledgements. The author wishes to thank Robin Cockett for interesting discussions on the category theory of distributive categories, and applications. Similarly, thanks are due to Samson Abramsky and Bob Coecke for many discussions on the interpretation of distributivity and the direct sum, and on categorical quantum mechanics generally. Thanks are also due to Philip Scott, for discussions and references on categorical models of linear logic, with particular reference to the treatment of both distributivity and models of Girard's bang !( ) operation.

An Apology. The work in this paper was first presented at a QICS quantum computing conference (Oxford 2010), under the title *'The role of coherence in quantum algorithms'* (*http://www.comlab.ox.ac.uk/quantum/content/1005021/*).

After the talk, the speaker was approached by a delegation of experimental physicists, who explained that they had attended the talk because of the mention of 'coherence' in the title, in the hope that it would be a break from the hard-core category theory presented in other talks. The author wishes to apologise for the (intentionally) misleading title, but hopes that they enjoyed the talk nevertheless.

References

1. Abramsky, S., Coecke, B.: A categorical semantics of quantum protocols. In: Proc. 19th Annual IEEE Symp. on Logic in Computer Science (LICS 2004), pp. 415–425. IEEE Computer Soc. Press (2005)
2. Abramsky, S.: Abstract Scalars, Loops, and Free Traced and Strongly Compact Closed Categories. In: Fiadeiro, J.L., Harman, N.A., Roggenbach, M., Rutten, J. (eds.) CALCO 2005. LNCS, vol. 3629, pp. 1–29. Springer, Heidelberg (2005)
3. Aharanov, D., Landau, Z., Makowsky, J.: The quantum FFT can be classically simulated, arXiv:quant-ph/0611156 v1 (2006)
4. Barr, M.: Algebraically Compact Functors. Journal of Pure and Applied Algebra 82, 211–231 (1992)
5. Blute, R.F., Cockett, J.R.B., Seely, R.A.G., Trimble, T.H.: Natural deduction and coherence for weakly distributive categories. Mathematical Structures in Computer Science 113, 229–296 (1991)
6. Carboni, A., Lack, S., Walters, R.: Introduction to Extensive and Distributive Categories. Journal of Pure and Applied Algebra 84, 145–158 (1993)
7. Cockett, J.R.B.: Introduction to Distributive Categories. Mathematical Structures in Computer Science 3, 277–307 (1993)
8. Coecke, B., Pavlovic, D.: Quantum measurements without sums. In: Chen, G., Kauffman, L., Lamonaco, S. (eds.) Mathematics of Quantum Computing and Technology. Taylor and Francis (arxiv.org/quant-ph/0608035) (2007)
9. Hines, P.: Quantum circuit oracles for abstract machine computations. Theoretical Computer Science 411, 1501–1520 (2010)
10. Høyer, P., Špalek, R.: Quantum Fan-out is Powerful. Theory of Computing 1(5), 81–103 (2005)
11. Joyal, A., Street, R.: The geometry of tensor calculus. Advances in Mathematics (102), 20–78 (1993)
12. Joyal, A., Street, R.: The geometry of tensor calculus II (manuscript)
13. Laplaza, M.: Coherence for categories with associativity, commutativity, and distributivity. Bulletin of the American Mathematical Society 72(2), 220–222 (1972)
14. Laplaza, M.: Coherence for distributivity. In: MacLane, S. (ed.) Coherence in Categories. Springer Lecture Notes in Mathematics, vol. 281, pp. 29–65 (1972)
15. MacLane, S.: Duality for groups. Bulletin of the American Mathematical Society 56(6), 485–516 (1950)
16. MacLane, S.: Categories for the working mathematician, 2nd edn. Springer, New York (1998)

17. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
18. Pati, A., Braunstein, S.: Impossibility of deleting an unknown quantum state. Nature 404, 164–165 (2000)
19. Shor, P.: Algorithms for quantum computation: discrete log and factoring. In: Proceedings of IEEE FOCS, pp. 124–134 (1994)
20. Wootters, W., Zurek, W.: A Single Quantum Cannot be Cloned. Nature 299, 802–803 (1982)
21. Yoran, N., Short, A.: Classical simulability and the significance of modular exponentiation in Shor's algorithm, arXiv:quant-ph/0706.0872 v1 (2007)