2013 28th Annual ACM/IEEE Symposium on Logic in Computer Science

Topological Structure of Quantum Algorithms

Jamie Vicary

Centre for Quantum Technologies
National University of Singapore
jamie.vicary@nus.edu.sg

Department of Computer Science
University of Oxford, UK
jamie.vicary@cs.ox.ac.uk

***Abstract*—We use a categorical topological semantics to examine the Deutsch-Jozsa, hidden subgroup and single-shot Grover algorithms. This reveals important structures hidden by conventional algebraic presentations, and allows novel proofs of correctness via local topological operations, giving for the first time a satisfying high-level explanation for why these procedures work. We also investigate generalizations of these algorithms, providing improved analyses of those already in the literature, and a new generalization of the single-shot Grover algorithm.**

***Index Terms*—quantum computing, quantum algorithms, topology, category theory**

I. Overview

A. Introduction

Important quantum procedures often seem mysterious because of the low-level way in which they are presented. A direct description of the required state preparations, unitary operators and projective measurements in terms of matrices of complex numbers gives exactly the required information to actually implement a particular protocol — but almost no information about why it should work.

One reason for this is that quantum information has a *topological* nature. The overall effect of a composite of quantum operations depends not so much on the order of composition, as on the topological flows of information that this induces, as demonstrated in striking fashion by Abramsky, Coecke et al [1, 2, 6, 7, 8, 9, 10, 11, 12, 19, 23], in a body of work that comprises the Categorical Quantum Mechanics research programme. Their topological semantics de-emphasize the matrices of complex numbers used in conventional presentations of quantum procedures, replacing them with geometrical primitives that give a satisfying explanation for why these procedures work. This provides a mature set of tools for analyzing a wide range of quantum procedures, especially those which make use of Bell-type entanglement or complementary observables.

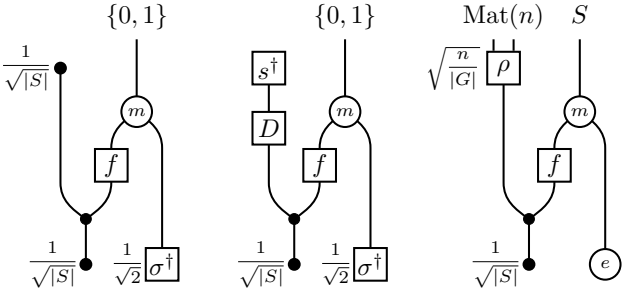
However, this research programme has not yet provided a topological analysis of the most important quantum *algorithms* (although see [19] for interesting work along these lines.) Quantum algorithms can be usefully distinguished from quantum *procedures* such as quantum teleportation, dense coding or key exchange, which bring about a certain physical effect rather than compute a particular quantity. Features of quantum algorithms that make them hard to model using the topological formalism include the use of an oracle and a reliance on group representation theory.

This paper overcomes these difficulties, providing a topological account of the Deutsch-Jozsa, hidden subgroup and single-shot Grover algorithms. This gives a consistent, high-level structural account of why these important quantum algorithms work, directly exposing the relevant flows of quantum information, and allowing new proofs of correctness.

This new perspective makes it much easier to consider generalizations of these algorithms. For the single-shot Grover algorithm, this generalization appears to be new. While the traditional Grover algorithm is based on the group $\mathbb{Z}_2$, our generalization is based on an arbitrary finite group G. Given a set coloured by the elements of G in a particular ratio, the algorithm identifies with a single query an element with an infrequent colour. To give a concrete example, consider a basket of red, blue and green balls, promised to be coloured in the ratio 4:1:1 in some order. For $G = \mathbb{Z}_3$ the generalized Grover algorithm will identify one of the less frequently–occurring colours with a single query, a task that cannot be achieved with the ordinary Grover algorithm.

The literature already contains descriptions of generalized Deutsch-Jozsa [14, 17] and hidden subgroup [13] algorithms. As with the original algorithms, these generalizations are technically opaque, and require long proofs which provide relatively little insight. We obtain new descriptions of these generalized algorithms using our topological techniques, giving a clear view of their structure, and simpler proofs of correctness. For the Deutsch-Jozsa algorithm, this clarity allows us to produce a new generalization that goes beyond that given in the literature.

The topological forms of the Deutsch-Jozsa, hidden subgroup and single-shot Grover algorithms that we develop are summarized by the following diagrams:



Deutsch-Jozsa **Single-shot Grover** **Hidden subgroup**

Each diagram represents an entire protocol, including the state preparation, unitary dynamics and measurement stages. We

1043-6871/13 $26.00 © 2013 IEEE
DOI 10.1109/LICS.2013.14

use the word 'topological' to describe our approach since it is based on an existing topological notation for the linear algebra of finite groups and sets, which is summarized for easy reference in Appendix I. We explore the three algorithms in Sections II, III and IV respectively.

Acknowledgements: This project grew out of discussions with Bob Coecke. I am grateful to John Baez, Bob Coecke, Brendan Fong and William Zeng for useful comments. Diagrams have been produced using the package *TikZ*.

B. Shortcomings of the circuit notation

We begin by outlining the usual circuit-based presentation of the Deutsch-Jozsa algorithm, as can be found in standard reference texts such as [18]. Presented in this manner the algorithm seems an idiosyncratic collection of individual parts, which come together to solve the Deutsch-Jozsa problem in an apparent minor miracle. In contrast, the new topological presentation we develop in Section II shows the consistent structure that lies hidden beneath each part of the algorithm. Not all descriptions of the Deutsch-Jozsa algorithm have the shortcomings we describe here, but all of them are commonly encountered.

The conventional Deutsch-Jozsa algorithm involves a function

$$\{0,1\}^N \xrightarrow{f} \{0,1\}, \tag{1}$$

where $\{0,1\}$ is the group of integers under addition modulo 2, and $\{0,1\}^N$ is the N-fold cartesian product of this group for some natural number N. This function is promised to have one of two properties: it is either *constant*, meaning that it takes the same value on every element of S; or *balanced*, meaning that it takes each possible value on exactly half of the elements of S. This gives us a first question:

Why should "constant" or "balanced" be important properties?

We then construct a unitary operator

$$(\mathbb{C}^2)^N \otimes \mathbb{C}^2 \xrightarrow{U_f} (\mathbb{C}^2)^N \otimes \mathbb{C}^2 \tag{2}$$

from our function f, which is defined to act in the following way:

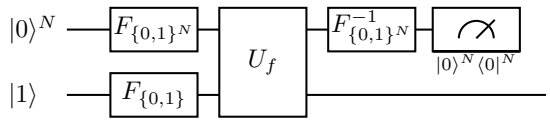
$$|k\rangle \otimes |b\rangle \xmapsto{U_f} |k\rangle \otimes |b \oplus f(k)\rangle \tag{3}$$

Here k is an element of $\{0,1\}^N$, and b is an element of $\{0,1\}$. The symbol $\oplus$ represents addition modulo 2, which is the group structure on $\{0,1\}$. This poses another question:

Does the group structure on $\{0,1\}^N$ play an essential role?

It has not been relevant so far, in the definitions of constant or balanced function or in the definition of U_f.

We then build the following quantum circuit:



(4)

We read this from left to right, as is conventional for quantum circuit diagrams. We begin by preparing N qubits in the state $|0\rangle$, and a single qubit in the state $|1\rangle$. We then apply the unitary operators $F_{\{0,1\}^N}$ and $F_{\{0,1\}}$, representing the Fourier transform operations on the groups $\{0,1\}^N$ and $\{0,1\}$ respectively. The operator U_f is then applied, followed by an inverse Fourier transform $F^{-1}_{\{0,1\}^N}$ on the upper family of N qubits, and a projective measurement onto the state $|0\rangle^N$. The lower qubit plays no role after the application of the unitary U_f.

This seems to suggest that the group structure on $\{0,1\}^N$ is relevant after all, since it is used to construct the Fourier transform operator $F_{\{0,1\}^N}$. Other descriptions of the Deutsch-Jozsa algorithm involve an application of the N-fold Hadamard gate $H^{\otimes N}$, but this again implies the codomain of f is of the form $\{0,1\}^N$. However, we only apply this operator to the element $|0\rangle^N$, which represents the identity element of the group. On this element, the Fourier transform acts as follows, creating an even superposition of the group elements:

$$F_{\{0,1\}^N}(|0\rangle^N) = \frac{1}{\sqrt{2^N}} \sum_{k \in \{0,1\}^N} |k\rangle \tag{5}$$

But this superposition is *independent* of the group structure, since the Fourier transform on any abelian group gives this result on the identity element. The application of $F^{-1}_{\{0,1\}^N}$ at the end of the protocol is insensitive to the group structure for the same reason, since it is followed by a projective measurement onto the state $|0\rangle^N$, and hence its sole function is to allow an effective projective measurement onto the same superposition state (5).

Further questions are also raised by the quantum circuit given above.

Why should we prepare the upper qubits in the state $|0\rangle^N$?

A partial answer to this question is given by the reasoning above: by the action of the Fourier transform, it allows us to access an even superposition of every element of $\{0,1\}^N$, and hence, in some sense, probe our function f on "every input simultaneously". But this is a vague notion: for what high-level reason should it enable the protocol to succeed? We can ask a similar question for the lower qubit:

Why should we prepare the lower qubit in the state $|1\rangle$?

The Fourier transform $F_{\{0,1\}}$ acts on this state to produce the superposition $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Why should this be the correct state to feed into the operator U_f?

The last step of the algorithm is to perform a projective measurement on the upper family of qubits onto the state $|0\rangle^N$. As discussed, given that this follows an application of the inverse Fourier transform $F^{-1}_{\{0,1\}^N}$, the overall effect is to measure the qubits in the state (5). If the projective measurement is successful, then we can conclude with certainty that our original function f is balanced. If the measurement fails, then we can conclude with certainty that f is constant.

Some further questions naturally raise themselves here.

Why should we measure the upper qubits in the state $|0\rangle^N$?

Why should we expect the measurement to succeed or fail exactly when the original function was constant or balanced?

Should measurement on the second family of qubits play a role?

A high-level understanding of the Deutsch-Jozsa algorithm will provide good answers to all these questions, as we see in the next section.

More ambitiously, we could also ask the following final question.

Can this algorithm be generalized?

This traditional presentation gives no indication as to whether this is the case. In fact, there is a broad class of possible generalizations, and their structure emerges naturally from our new topological approach.

II. Topological Deutsch-Jozsa

A. Introduction

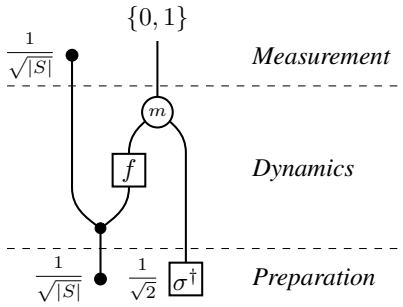
We now present a new topological perspective on the Deutsch-Jozsa algorithm, making use of the topological formalism for algebra introduced in Appendix I. This formalism will make clear many of the mysterious features of the traditional presentation of the algorithm, as highlighted in the account in Section I-B, by showing how the functionality of the algorithm is enabled by its topological structure.

The traditional presentation focused on properties of a function $\{0,1\}^N \xrightarrow{f} \{0,1\}$ between abelian groups. However, we argued that at no point in the protocol was the group structure on $\{0,1\}^N$ used in an essential way. For this reason, in our new perspective, we redefine our function to be of type

$$S \xrightarrow{f} \{0,1\} \tag{6}$$

where S is a finite set.

The overall structure of the algorithm is given by the topological diagram below, in which time flows from bottom to top. The preparation, unitary dynamics and measurement phases are clearly indicated.



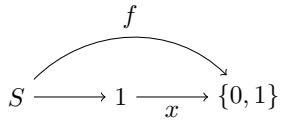
(7)

Over the course of this section we explain why this diagram represents the conventional Deutsch-Jozsa algorithm, and show how its form gives rise to a topological proof of correctness.

We then show how we can replace the group $\{0,1\}$ by an arbitrary finite group, and obtain a natural generalization of the Deutsch-Jozsa procedure. The algorithm we describe is close to that of Batty, Braunstein, Duncan and Høyer [14, 17], but strictly more general. The topological approach gives rise to a new proof of correctness, which is both shorter and more structurally informative than that allowed by the original approach.

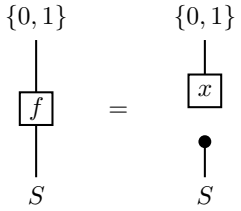
B. Constant and balanced functions

For the function $S \xrightarrow{f} \{0,1\}$ to be *constant* means that it must factor via the 1-element set:



(8)

The function $S \to 1$ is the unique function to the 1-element set, and the function $1 \xrightarrow{x} \{0,1\}$ selects the element of $\{0,1\}$ which is the image of the function f. Linearizing these functions to produce linear maps between the free vector spaces on the original sets, expression (8) has the following graphical representation:



(9)

The function f is constant iff there exists some function x satisfying this condition.

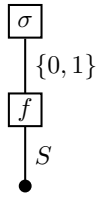
We now consider the case that f is balanced, meaning it takes each possible value on an equal number of elements of its domain. We can express this condition with the following equation:

$$\begin{pmatrix} 1 & -1 \end{pmatrix} \circ \sum_{s \in S} |f(s)\rangle = 0 \tag{10}$$

Here we have composed with the matrix $\{0,1\} \xrightarrow{(1\ -1)} \mathbb{C}$, which contributes $+1$ to the sum for each element $s \in S$ with $f(s) = |0\rangle$, and -1 for each element with $f(s) = |1\rangle$. So it is clear the sum is zero exactly when f is balanced. We can reexpress this equation as follows:

$$\begin{pmatrix} 1 & -1 \end{pmatrix} \circ f \circ \sum_{s \in S} |s\rangle = 0 \tag{11}$$

We can express this graphically using our topological formalism, where we write σ for the linear map $\{0,1\} \xrightarrow{(1\ -1)} \mathbb{C}$, which is in fact the alternating representation of the group:

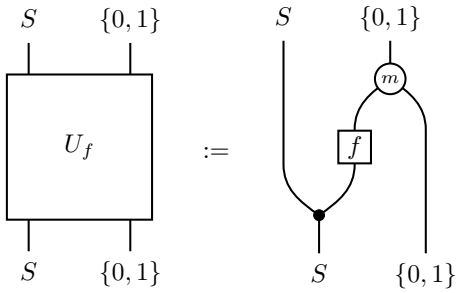


$$= \quad 0 \tag{12}$$

Equations (9) and (12) can thus serve to replace the constant and balanced properties, giving us entirely topological conditions on the function f.

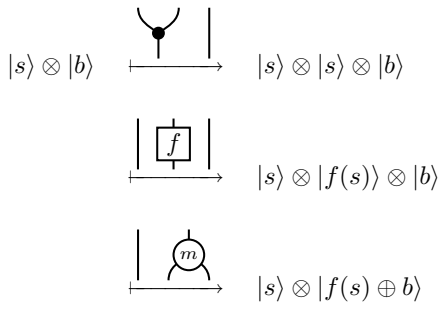
C. Building the unitary

At the heart of the Deutsch-Jozsa algorithm is the unitary operator U_f, with action defined by expression (3). We can define this topologically as follows:



(13)

To show this acts in the correct way, we evaluate its effect on a general input element, for some choice of $s \in S$ and $b \in \{0,1\}$:

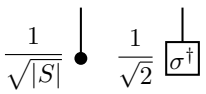


(14)

This matches our earlier definition (3).

D. Performing the algorithm

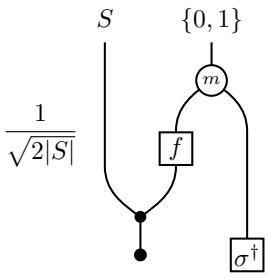
To obtain a topological expression for the result of the algorithm, we precompose expression (13) with the choice of input state. The input states have the following graphical form:



(15)

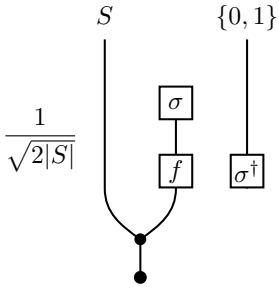
This expression includes the action of the Fourier transform operations on the input states of the traditional Deutsch-Jozsa circuit (4), which as we remarked in Section I-B have the effect of preparing the equal superposition state and the adjoint of the irreducible representation σ, up to a normalizing factor.

By composing expressions (15) and (13) we obtain the following topological expression for the quantum state after the protocol has been implemented, but before any measurement is performed:



(16)

We omit the inverse Fourier transform present in the traditional circuit diagram (4) as we view it as forming part of the measurement. Due to property (82) of the multiplication vertex, we can rewrite this to obtain the following equivalent expression:



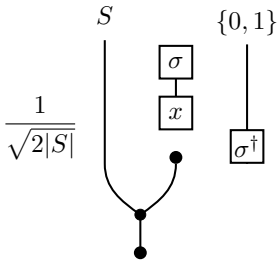
(17)

This looks superficially different to equation (82) only because the representation is 1-dimensional, and so the intermediate wires become trivial.

We see that the quantum state becomes a product state. We now examine the effect of a measurement on this state in the case that the function f is constant or balanced.

E. Result when f is constant

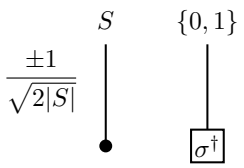
When f is constant, we apply the topological equation (9) to rewrite expression (17) for the quantum state after the unitary evolution stage of the algorithm has been completed, obtaining the following diagram:



(18)

The composite $\sigma \circ x$ represents the value of the irreducible representation σ on the element $x \in \{0,1\}$ which is the image of the function f. Since $\sigma = (\,1 \;\; -1\,)$, this composite equals ± 1. Using this fact, along with the properties of the topological algebra on a finite set, we simplify diagram (18)

to obtain the following expression:

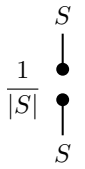


(19)

This is a product state, with the left-hand family of qubits in the superposition state (5). As a result, the projective measurement performed onto the superposition state is guaranteed to be successful. This demonstrates that, in the case that f is constant, we will measure the system S to be in the superposition state (5) with certainty.

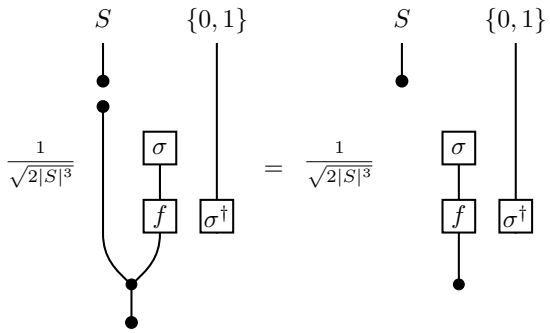
F. Result when f is balanced

We now consider the result of a measurement of the left-hand system in the superposition state (5) in the case that f is balanced. The following diagram represents a projector onto the 1-dimensional subspace of S corresponding to the uniform superposition state:



(20)

Postcomposing this with expression (17) representing the quantum state after the main body of the algorithm has been performed, and then simplifying the result, we obtain the following diagram:



(21)

By equation (12) defining the case when f is balanced, we see that this composite is equal to 0. We conclude that there is no probability of measuring the system to be in the uniform superposition state (5). This completes the topological demonstration of correctness of the Deutsch-Jozsa algorithm.

G. Generalization to arbitrary finite groups

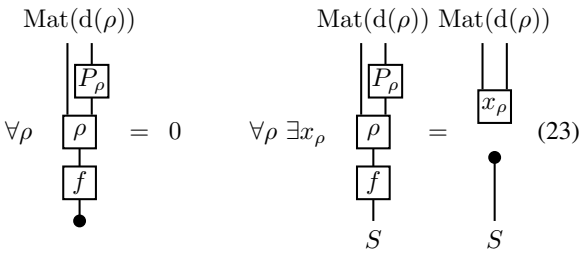
Our topological approach allows the Deutsch-Jozsa to be easily generalized from the group $\{0, 1\}$ to an arbitrary finite groups G, with the function then having the type

$$S \xrightarrow{f} G. \tag{22}$$

In the traditional Deutsch-Jozsa algorithm described earlier in this section, the alternating representation $\{0, 1\} \xrightarrow{\sigma} \mathbb{C}$ plays a central role. In this generalization we replace it with an arbitrary irreducible representation $G \xrightarrow{\rho} \mathrm{Mat}(n)$, where n is the dimension of the representation. We continue our convention of viewing the symbol G as representing both a finite group and the free vector space $\mathbb{C}[G]$ depending on context. The concepts of constant and balanced functions will also be generalized, in a way which we will see below.

The generalization of the Deutsch-Jozsa algorithm presented here is closely related to that of Batty, Braunstein, Duncan and Høyer [14, 17]. We believe our formulation is strictly more general. In addition, thanks to the topological calculus, the proof of correctness is only a couple of pages, rather than the many pages required in these references. The topological formalism also makes it clear exactly *why* the generalized algorithm is successful.

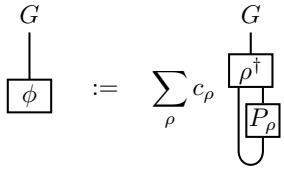
We begin by defining generalizations of the constant and balanced properties. For each isomorphism class of irreducible representation ρ, in which the group acts on the Hilbert space V_ρ, we pick an orthogonal projector $V_\rho \xrightarrow{P_\rho} V_\rho$ onto some subspace, such that at least one of these projectors is nonzero. With respect to such a family P_ρ of projectors, we make the following definitions of the properties P_ρ-*balanced* and P_ρ-*constant*:



(23)

P_ρ-balanced $\qquad$ P_ρ-constant

We then define an element ϕ of the group algebra of G in the following way:

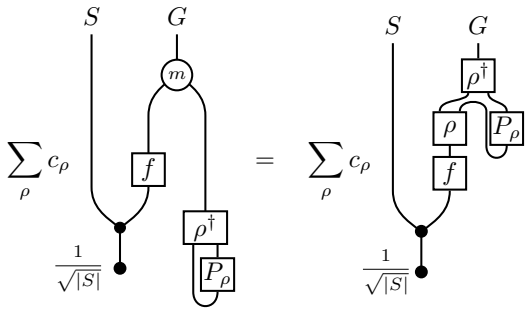


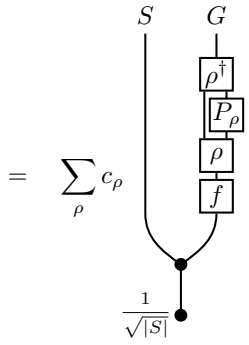
(24)

The summation is over the equivalence classes of irreducible representations ρ of G. The coefficients c_ρ are arbitrary but nonzero, and can always be picked to ensure that ϕ has norm 1. It is here that our procedure is more general than that of Batty, Duncan and Braunstein [17], who require a single P_ρ to have trace 1, and all others to have rank 0. Also, they require the nonzero projector to have support given by a particular basis element of the representation space.

Our generalized Deutsch-Jozsa algorithm proceeds as in the standard case described earlier in this section, except we use this state ϕ as the initial state for the system G. After the unitary dynamics step, the state of the system has the following

topological form:

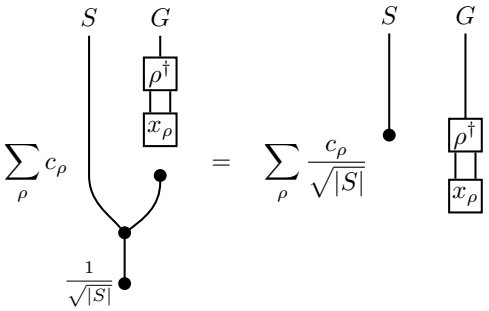




(25)

We are now ready to consider the measurement stage of the protocol, which is a projective measurement onto the even superposition state of S.

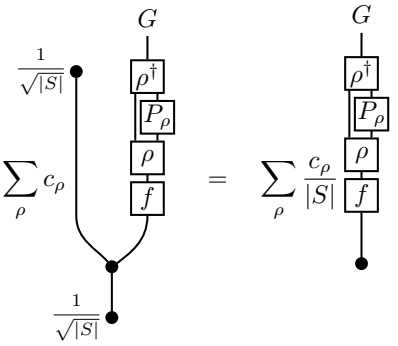
Suppose that f is P_ρ-constant. Then using equation (23) we obtain the following expression for the overall state of the joint system:



(26)

This is a product state, with the system S in the even superposition state. It is not the zero state, since the maps $\rho^\dagger$ are injective, and at least one x^ρ is nonzero. A projective measurement of S onto the even superposition state is therefore guaranteed to be successful.

Finally, suppose that f is P_ρ-balanced. To determine the effect of a projective measurement onto the even superposition state, we compose (38) with a partial isometry onto that subspace of the system S:



(27)

Using the definition (23) of a P_ρ-balanced function, this composite is zero, so we have shown that in the P_ρ-balanced case there is no possibility of measuring the system S in the even superposition state.

III. The Single-Shot Grover Algorithm

A. Introduction

In this section we give a topological analysis of the single-shot Grover algorithm, which is used to search a set S for marked elements, defined in terms of an indicator function

$$S \xrightarrow{f} \{0, 1\}$$

onto the group of integers under addition modulo 2. Grover's algorithm is nondeterministic in general, which makes it difficult to treat in our formalism. We restrict attention to the single-shot case in which a single iteration of the algorithm is guaranteed to return a marked element. This corresponds to the case that exactly $\frac{1}{4}$ of the elements are marked. Our topological analysis makes it clear why Grover's algorithm is always successful in this case.

We then explore a generalization of Grover's algorithm, made natural by our approach, in which our set S is equipped with a function to an arbitrary finite group. We demonstrate that this generalized algorithm is guaranteed to return an *unbalanced* element of S after a single iteration. Given an irreducible representation ρ of G, we define the element $s \in S$ to be *balanced* if the following holds:

$$\rho(f(s)) = \frac{2}{|S|} \sum_{t \in S} \rho(f(t)) \tag{28}$$

In words, an element $s \in S$ is balanced if $\rho(f(s))$ equals twice the average value, using the uniform measure on S. If an element is not balanced, then it is *unbalanced*.

To illustrate this, consider the case of $G = \mathbb{Z}_3$, and write $\underline{6}$ for the set $\{1, 2, 3, 4, 5, 6\}$. Consider the function $\underline{6} \xrightarrow{f} \mathbb{Z}_3$ defined as follows:

$$f(1) = 0 \qquad f(5) = 1 \qquad f(6) = 2$$
$$f(2) = 0$$
$$f(3) = 0$$
$$f(4) = 0$$

We choose the representation $\mathbb{Z}_3 \xrightarrow{\rho} \mathbb{C}$ with $\rho(1) = e^{2\pi i/3}$. Under this representation, the average value of the quantity $\rho(f(n))$ over all $n \in [6]$ is

$$\frac{1}{6}(4 + e^{2\pi i/3} + e^{-2\pi i/3}) = \frac{1}{2}. \tag{29}$$

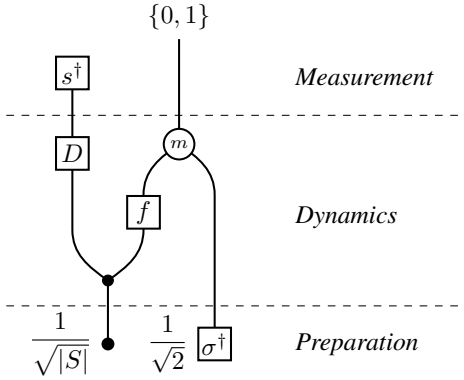
As a result, the elements 1, 2, 3 and 4 are balanced, since for these values $\rho(f(n))$ takes the value 1 which is twice the average value. The elements 5 and 6 are unbalanced, so these are the only possible measurement outcomes, and the algorithm will determine one of them in a single query.

This works for any function $f : S \to \mathbb{Z}_3$, for any set S, as long as it takes the values of $\mathbb{Z}_3$ in the ratio $4 : 1 : 1$ in some order. In this general case, as with the simpler scenario we examined above, the algorithm will return an element of S marked with one of the less-frequent values of $\mathbb{Z}_3$ in a single query.

We emphasize that this cannot be handled by the standard Grover algorithm. If we knew beforehand what values of G are taken by the unbalanced elements of S (in our simple example, 1 and 2), and if we knew the fraction of elements which are unbalanced (in this case $\frac{1}{3}$), then we could compose f with a function to $\mathbb{Z}_2$ that takes $0 \mapsto 0$, $1 \mapsto 1$ and $2 \mapsto 1$, and apply an optimal variant of Grover's conventional search algorithm to find a rare element with certainty after a single iteration [5]. However, in general, this information may not be known.

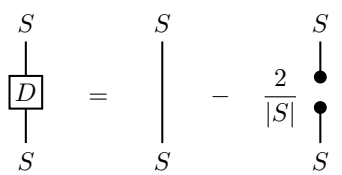
B. Topological presentation

Our topological perspective demonstrates why the single-shot Grover algorithm is successful, when exactly a quarter of the elements are marked. The overall topological structure of the algorithm is as follows:



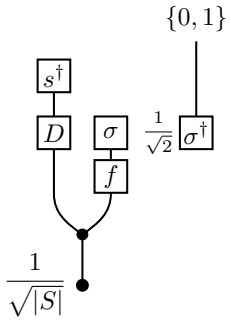
(30)

This represents the final state after a successful projective measurement of the first system in the basis state $|s\rangle$. Furthermore, we can decompose D in the following way, as a linear combination of two other diagrams:



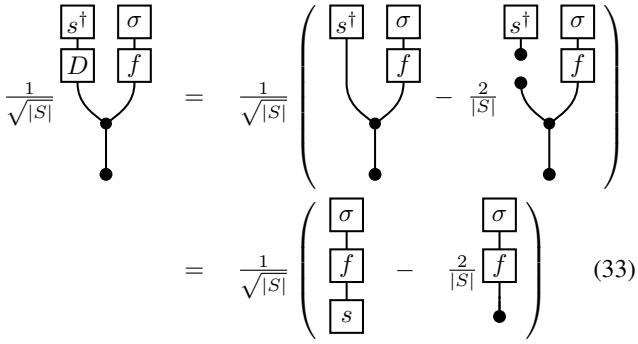
(31)

This linear decomposition allows us to perform a completely topological analysis of the algorithm. By equation (82), the linear map $\sigma^\dagger$ is duplicated by the group multiplication vertex m in equation (35), allowing us to rewrite it in the following way:



(32)

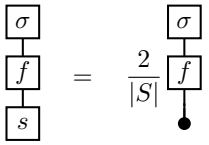
Since this is a product state, we can neglect the second system, rewriting the state of the first system using the topological decomposition (31) of the diffusion operator D:



(33)

In the final equality we use properties of the topological algebra of finite sets, as described in Sections I-C and I-D.

This is zero for those $s \in S$ satisfying the following equation:



(34)

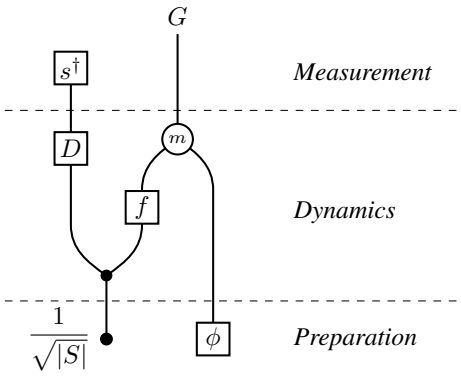
Such an s cannot be the result of a measurement. The right-hand side of this expression represents twice the average value of the function f under the representation σ. The left-hand side represents the value of the function f at the element s, under the representation σ. If the right-hand side is equal to $+1$, it is straightforward to see that f must take the value 1 on three-quarters of the elements of S. If the right-hand side is equal to -1, then f must take the value 1 on one-quarter of the elements of S.

This recovers the standard result from Grover search: to find a marked element with certainty after a single step, exactly a quarter of elements must be marked. Note that standard Grover theory assumes that the marked elements take the value 1 under the function f, but this is not required: the marked elements could just as well take the value 0, and the ummarked

elements the value 1. It is clear that these two cases give rise to essentially the same procedure, since the difference corresponds to an overall phase. So one can argue that the traditional Grover algorithm should not be thought of as a search algorithm, but as a 'frequency detection' algorithm, an idea which fits well with our generalized versions.

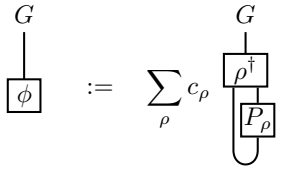
C. Generalization

We generalize this by replacing the group $\{0, 1\}$ with an arbitrary finite group G. Loosely, the generalized algorithm is guarantees to find an element $s \in S$ for which $\rho(f(s))$ does not take twice its average value, restricted to some chosen subspace of the representation space. The following diagram gives a topological outline of the algorithm:



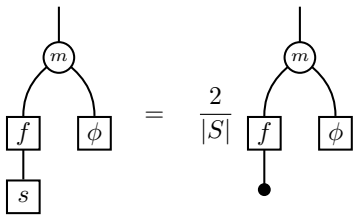
(35)

The system G is initialized in a state ϕ which is chosen in the following way, just as with the generalized Deutsch-Jozsa algorithm presented in Section II-G:



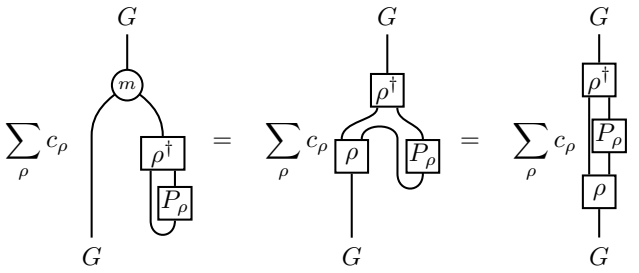
(36)

By following a similar argument to the previous section, we obtain the following expression for the basis elements $|s\rangle \in S$ which have zero amplitude to be measured:



(37)

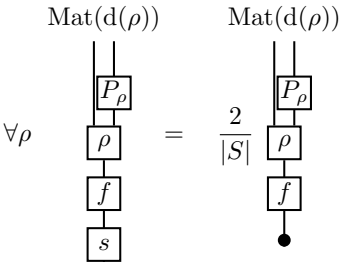
From this equation, we see that the algorithm will never return those elements $s \in S$ such that, restricted the support of $m(-, \phi)$, the group element $f(s)$ takes twice its average value. We can apply definition (36) to see how $m(-, \phi)$ acts in terms of our chosen projectors P_ρ:



(38)

The support of this operator is the union of subspaces defined by our projectors P_ρ, across all the equivalence classes of irreducible representations.

Applying this to equation (37), we see that a basis element $|s\rangle \in S$ cannot be the result of the measurement if it satisfies the following condition, which generalizes condition (34) above for a balanced element of S:



(39)

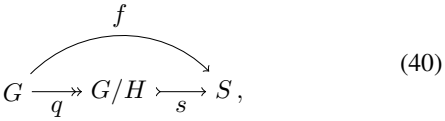
This says that, under each representation ρ, restricted to the subspace $\mathrm{id}_{\mathrm{d}(\rho)} \otimes P_\rho$, the group element $f(s)$ takes twice its average value.

IV. The hidden subgroup algorithm

A. Introduction

The hidden subgroup family of algorithms is rich, containing Deutsch's original algorithm, as well as Simon's algorithm and Shor's algorithm. We use our topological notation to prove correctness of the algorithm, and clarify its structure.

We are given a function $G \xrightarrow{f} X$, promised to be constant on the cosets of some normal subgroup $H \subseteq G$, and distinct otherwise. This says exactly that the function f factorizes as



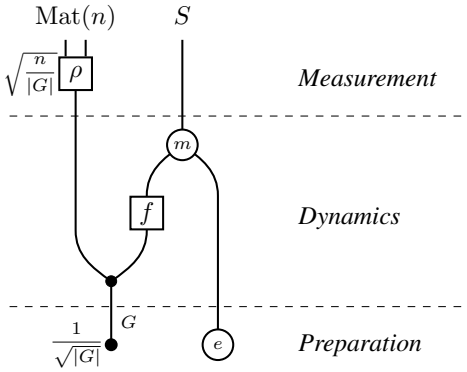
(40)

where q is a surjective projection onto the quotient group G/H, and s is an embedding into some set. The algorithm determines the subgroup H in $O(\log |G|)$ trials.

Traditionally applied only in the case where G is abelian, it was extended to the case of normal subgroups of arbitrary finite groups by Hallgren, Russell and Ta-shma [13]. It is this generalized version that we treat here. Our approach gives a clean separation between the group-theoretical and quantum aspects of the protocol, and yields a proof of correctness which is simpler, shorter, and easier to follow.

B. Topological version

The following diagram summarizes our topological account of the algorithm.

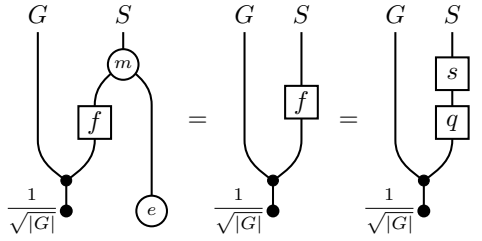


(41)

We begin by preparing two systems: one with state space given by a group algebra G in the uniform superposition state; and another with state space given by a set S in some basis state $|e\rangle$. We then perform the unitary dynamics described by the second section, which as described in Section II-C recreates the action of the unitary operator U_f in the conventional presentation. For this purpose we require a group structure on S; we choose any structure (such as a cyclic group structure) such that e is the identity element.

The procedure finishes with a measurement on the first system in the partition defined by the irreducible representations, as described in Section I-H. Using a topological encoding of a result from group theory, we demonstrate that the only representations that can be successfully measured are those which arise as restrictions of representations of the quotient group G/H. Classical postprocessing then suffices to deduce the subgroup H in $O(\log |G|)$ trials [13].

After the unitary dynamics step, the systems are in the following state:



(42)

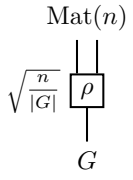
These are topological representations of the following algebraic expression:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \tag{43}$$

On the right-hand side of (42) we have rewritten f in terms of its promised factorization (40) via an unknown quotient group G/H.

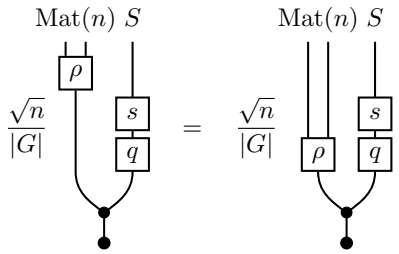
C. Performing the measurement

We now describe measurement of the first system G, using a projective measurement determined by the irreducible representations. To understand what results are possible, we compose the state (42) with the linear map



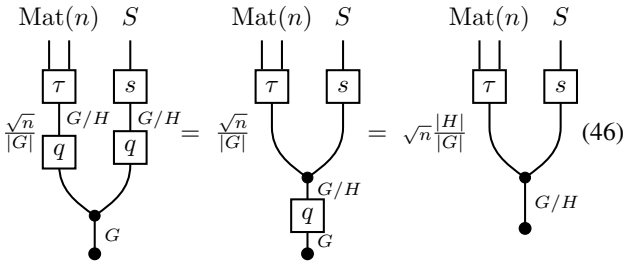
(44)

on the first factor, which as discussed in Section I-H is a partial isometry projecting onto the subspace of the group algebra corresponding to the irreducible representation ρ. This gives the following result:



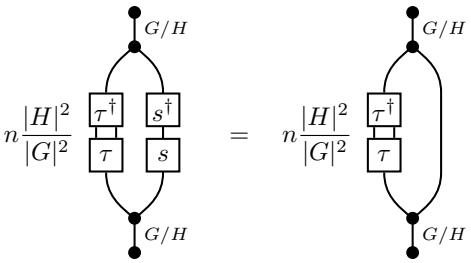
(45)

By Theorem I.3, this is zero exactly when ρ does not factor through the unknown quotient group G/H. So the only irreducible representations that can be measured in this way are those which factorize as $G \xrightarrow{q} G/H \xrightarrow{\tau} \mathrm{Mat}(n)$, for some irreducible representation τ of G/H. In this case, our projected state (45) can be rewritten as follows, making use of the topological properties of functions between basis elements and even surjections as presented in Section I-D:

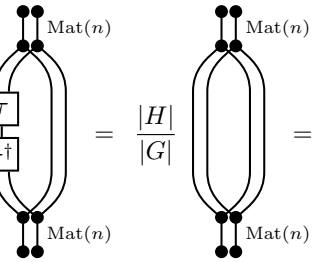


(46)

We calculate the norm of this vector in the following way, employing the graphical characterization of injective functions given in Section I-D, and both the cyclic property of the trace and the topological expression of the dimension of a vector space as developed in Section I-E:



$$= \; n\frac{|H|^2}{|G|^2} \; = \; \frac{|H|}{|G|} \; = \; \frac{|H|}{|G|}n^2 \qquad (47)$$



So the measurement will return exactly those irreducible representations of G that factor through the unknown quotient group G/H, with a probability proportional to the square of the dimension of the representation.

References

[1] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*, pages 415–425, 2004. IEEE Computer Science Press.

[2] Samson Abramsky and Bob Coecke. *Handbook of Quantum Logic and Quantum Structures*, volume 2, chapter Categorical Quantum Mechanics. Elsevier, 2008.

[3] John C Baez and Mike Stay. *New Structures for Physics*, chapter Physics, Topology, Logic and Computation: A Rosetta Stone, pages 95–172. Springer, 2010.

[4] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli. Clifford theory and applications. *Journal of Mathematical Sciences*, 156(1):29–43, 2009.

[5] Dong Pyo Chi and Jinsoo Kim. Quantum database search by a single query. *Lecture Notes in Computer Science*, 1509:148–151, 1999.

[6] Bob Coecke. The logic of entanglement: An invitation. Technical report, University of Oxford, 2003. Computing Laboratory Research Report PRG-RR-03-12.

[7] Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. *New Journal of Physics*, 13, 2011.

[8] Bob Coecke and Eric Oliver Paquette. POVMs and Naimark's theorem without sums. 2006.

[9] Bob Coecke, Eric Oliver Paquette, and Dusko Pavlovic. Classical and quantum structuralism. In Simon Gay and Ian Mackie, editors, *Semantic Techniques in Quantum Computation*, pages 29–69. Cambridge University Press, 2010.

[10] Bob Coecke and Dusko Pavlovic. *The Mathematics of Quantum Computation and Technology*, chapter Quantum Measurements Without Sums. Taylor and Francis, 2006.

[11] Bob Coecke, Dusko Pavlovic, and Jamie Vicary. Commutative dagger-Frobenius algebras in FdHilb are orthogonal bases. (RR-08-03), 2008. Technical Report.

[12] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. In *Proceedings of the 19th EACSL Annual Conference on Computer Science Logic*, number 6247 in Lecture Notes in Computer Science, 2010.

[13] Sean Hallgren, Alexander Russell, and Amnon Tashma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, 2000.

[14] Peter Høyer. Conjugated operators in quantum algorithms. *Physical Review A*, 59:3280–3289, 1999.

[15] Gregory M. Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[16] Joachim Kock. *Frobenius Algebras and 2D Topological Quantum Field Theories*. Cambridge University Press, 2004.

[17] Andrew J. Duncan Michael Batty and Samuel L. Braunstein. Extending the promise of the Deutsch-Jozsa-Høyer algorithm for finite groups. *Journal of Computation and Mathematics*, 9:40–63, 2006.

[18] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[19] Dusko Pavlovic. Geometry of abstraction in quantum computation. *arXiv:1006.1010*, 2010.

[20] Roger Penrose. Applications of negative-dimensional tensors. In D. J. A. Welsh, editor, *Combinatorial Mathematics and its Applications*. Academic Press, 1971.

[21] R. Rosebrugh, N. Sabadini, and R. F. C. Walters. Generic commutative separable algebras and cospans of graphs. *Theory and Applications of Categories*, 15(164–177):6, 2005.

[22] Peter Selinger. *New Structures for Physics*, chapter A Survey of Graphical Languages for Monoidal Categories, pages 289–355. Number 813 in Lecture Notes in Physics. Springer, 2011.

[23] Jamie Vicary. Higher semantics of quantum protocols. *Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science*, 2012. IEEE Computer Science Press, to appear.