Abstract structure of unitary oracles for quantum algorithms

William Zeng
Department of Computer Science, University of Oxford
william.zeng@cs.ox.ac.uk

Jamie Vicary
Centre for Quantum Technologies, University of Singapore
and Department of Computer Science, University of Oxford
jamie.vicary@cs.ox.ac.uk

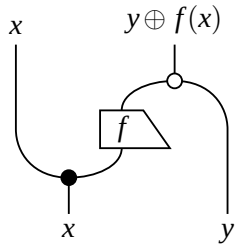
We show that a pair of complementary dagger-Frobenius algebras, equipped with a self-conjugate comonoid homomorphism onto one of the algebras, produce a nontrivial unitary morphism on the product of the algebras. This gives an abstract understanding of the structure of an oracle in a quantum computation, and we apply this understanding to develop a new algorithm for the deterministic identification of group homomorphisms into abelian groups. We also discuss an application to the categorical theory of signal-flow networks.

1 Introduction

1.1 Overview

Pairs of complementary dagger-Frobenius algebras play an important role in the high-level characterization of quantum phenomena [8, 13], as the algebraic content of mutually unbiased bases. In Section 2, we show that if a such a pair is equipped with a self-conjugate comonoid homomorphism onto one of the algebras, a *unitary* map can be constructed that has the same abstract structure as an *oracle* in the theory of quantum algorithms. This gives insight into the logical structure of quantum algorithms and opens up a new avenue for their generalization.

Most known quantum algorithms are constructed using these black-box quantum oracles, whose structure can be depicted graphically in the following way:



(1)

Here we read the diagram from bottom to top, defining a map of type $\mathbb{C}^n \otimes \mathbb{C}^m \to \mathbb{C}^n \otimes \mathbb{C}^m$ that acts as $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$ for a group product $\oplus$. Section 2 contains a full abstract description. Oracle-based algorithms include the Deutsch-Jozsa, Grover, and hidden subgroup algorithms. In the Deutsch-Jozsa and Grover algorithms the oracle implements a function $f : S \to \{0,1\}$ where S is a finite set. In the hidden subgroup algorithm, the oracle implements a function $f : G \to S$ where G is a finite group and S is a finite set. In [13] it was shown that the unitary oracle described in Section 2 characterizes the structure of these well-known algorithms.

For these oracles to be physically implementable, they must be *unitary operators*. In this paper we give an abstract proof of unitarity for these operators using categorical algebra. In Section 3 we apply

B. Coecke, I. Hasuo & P. Panangaden (Eds.):
Quantum Physics and Logic 2014 (QPL 2014).
EPTCS 172, 2014, pp. 270–284, doi:10.4204/EPTCS.172.19

this result to develop a new quantum algorithm for the identification of group homomorphisms into an abelian group, in a number of queries which is equal to the number of simple factors of the target group. The graphical approach provides a simple proof of correctness of the algorithm, and leads to an algorithm which is more general than existing work in the literature [11].

In Section 4 we investigate an application to the theory of signal-flow networks [2, 4, 10]. We show that the formalism contains dagger-Frobenius algebras equipped with self-conjugate homomorphisms, and that, as a consequence, the network representing a single resistor is unitary.

Acknowledgements. We are grateful to John Baez and Pawel Sobocinski for useful discussions about signal-flow networks. Section 4 of this paper has some technical overlap with [4] and was prepared independently. We are grateful to the authors for pointing out their work to us in the prepublication phase of this article. Will Zeng acknowledges the support of the Rhodes Trust in funding this work.

1.2 Frobenius monoids and complementarity

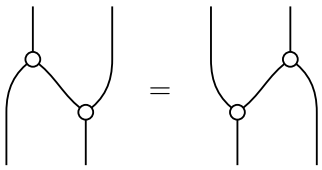
In this Section we collect some standard results from the literature [8]. We assume some familiarity with the graphical calculus for symmetric monoidal dagger-categories [12]. We use a notation in which morphisms are drawn from bottom-to-top.

Definition 1. In a monoidal category, a *comonoid* is a triple $(A,\curlyvee,\varrho)$ of an object A, a morphism $\curlyvee : A \to A \otimes A$ called the comultiplication, and a morphism $\varrho : A \to I$ called the counit, satisfying coassociativity and counitality equations:

(2)

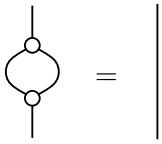
In a monoidal dagger-category, we can apply the dagger operation to these structures to obtain the associated monoid. We can then ask for the comonoid and monoid to interact in various ways.

Definition 2. In a monoidal dagger-category, a comonoid $(A,\curlyvee,\varrho)$ is *dagger-Frobenius* when the following equation holds:



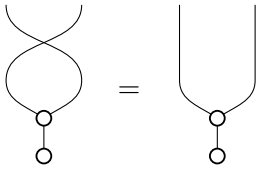
(3)

Definition 3. In a symmetric monoidal dagger-category, a *classical structure* is a commutative dagger-Frobenius comonoid $(A,\curlyvee,\varrho)$ satisfying the *specialness* condition:



(4)

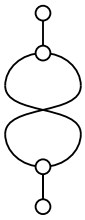
Definition 4. In a symmetric monoidal dagger-category, a dagger-Frobenius comonoid is *symmetric* when the following condition holds:



(5)

Definition 5. In a symmetric monoidal dagger-category, the *dimension* $d(A)$ of an object A equipped with a dagger-Frobenius comonoid $(A,\curlyvee,\varphi)$ is given by the following composite:

$\mathrm{d}(A) \quad :=$

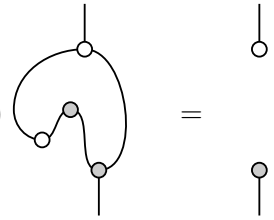


(6)

When the algebra is commutative and special, equation (6) can be simplified to the composition of the unit and counit.

Definition 6 (Complementarity)**.** In a symmetric monoidal dagger-category, two special symmetric dagger-Frobenius comonoids $(A,\curlyvee,\varphi)$ and $(A,\curlyvee,\varphi)$ are *complementary* when the following equation holds:

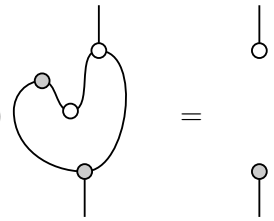
$\mathrm{d}(A)$



(7)

Note that this is not a symmetric condition between the gray and white structures. However, thanks to the symmetric property of the dagger-Frobenius algebras, it is equivalent to the following alternative condition:

$\mathrm{d}(A)$



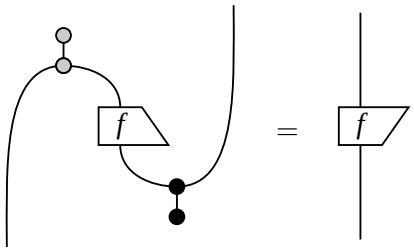
(8)

The daggers of these equations give rise to two further equivalent conditions.

By the symmetric property of the dagger-Frobenius algebras, this condition is equivalent to

Definition 7. In a monoidal dagger-category, a comonoid homomorphism $f : (A,\curlyvee,\bullet) \to (B,\curlyvee,\varphi)$

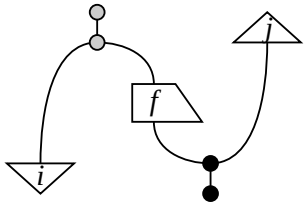
between dagger-Frobenius comonoids is *self-conjugate* when the following property holds:



(9)

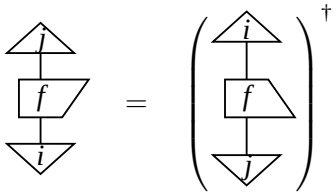
Lemma 8. *In* **Hilb**, *comonoid homomorphisms* $f : (A, \curlyvee, \bullet) \to (B, \curlyvee, \bullet)$ *of classical structures are self-conjugate.*

Proof. Recall that comonoid homomorphisms between classical structures in **Hilb** are exactly classical functions between the copyable points [9]. The linear maps on either side of (9) will be the same if and only if their matrix elements are the same, obtained by composing with $|i\rangle$ at the bottom and $\langle j|$ at the top. On the left-hand side, this gives the following result:



$$= \quad \begin{array}{c} i \\ f \\ j \end{array} \quad = \quad \begin{cases} 1 & \text{if } i = f(j), \\ 0 & \text{if } i \neq f(j). \end{cases} \tag{10}$$

On the right we can do this calculation:



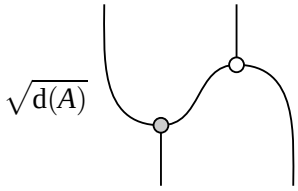
$$= \quad \left\{ \begin{array}{ll} 1 & \text{if } i = f(j) \\ 0 & \text{if } i \neq f(j) \end{array} \right\}^{\dagger} \quad = \quad \begin{cases} 1 & \text{if } i = f(j), \\ 0 & \text{if } i \neq f(j). \end{cases} \tag{11}$$

This is the same result as for the left-hand side, and so expression (9) holds. □

2 Unitary oracles

2.1 Complementarity via unitarity

A pair of symmetric dagger-Frobenius algebras can be used to build a linear map in the following way:

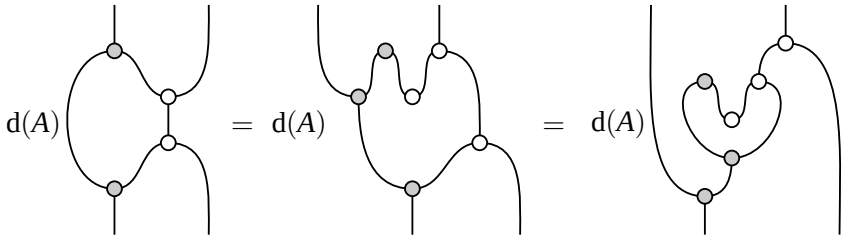


(12)

Here we have assumed that we operate in a category where square roots of scalars exist. The two algebras are complementary exactly when this composite is unitary, as we show in the following theorem.

Theorem 9 (Complementarity via a unitary)**.** *In a dagger symmetric monoidal category, two symmetric dagger-Frobenius algebras are complementary if and only if the composite* (12) *is unitary.*

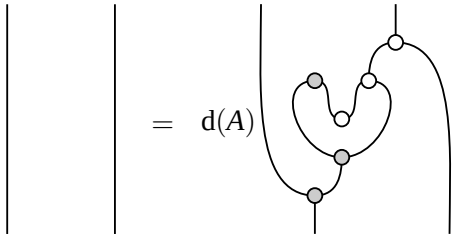
Proof. Composing (12) with its adjoint in one order, we obtain the following:



(13)

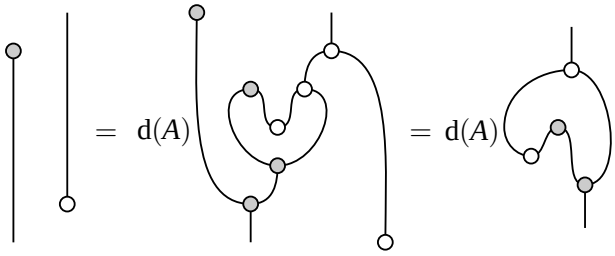
If the complementarity condition (7) holds then this is clearly the identity on $A \otimes A$. The other composite can be shown to be the identity in a similar way, and so (12) is unitary.

Conversely, suppose (12) is unitary. Then the final expression of (13) certainly equals the identity on $A \otimes A$:



(14)

Composing with the black counit at the top-left and the white unit at the bottom-right then gives back complementarity condition (7) as required:



(15)

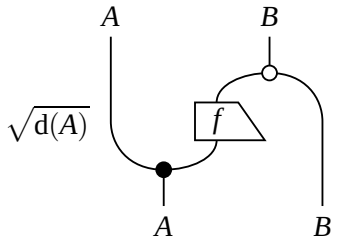
This completes the proof. □

2.2 Families of unitary oracles

This pair of complementary observables automatically gives rise to a much larger family of unitaries, one for each self-conjugate comonoid homomorphism onto one of the classical structures in the pair. See equation (9) for the definition of the self-conjugacy property. Lemma 8 demonstrated that in **FHilb**, every comonoid homomorphism of classical structures is self-conjugate.

Definition 10 (Oracle)**.** In a symmetric monoidal dagger-category, given a dagger-Frobenius comonoid $(A, \curlyvee, \blacklozenge)$, a pair of complementary symmetric dagger-Frobenius comonoids $(B, \curlyvee, \lozenge)$ and $(B, \curlyvee, \lozenge)$, and

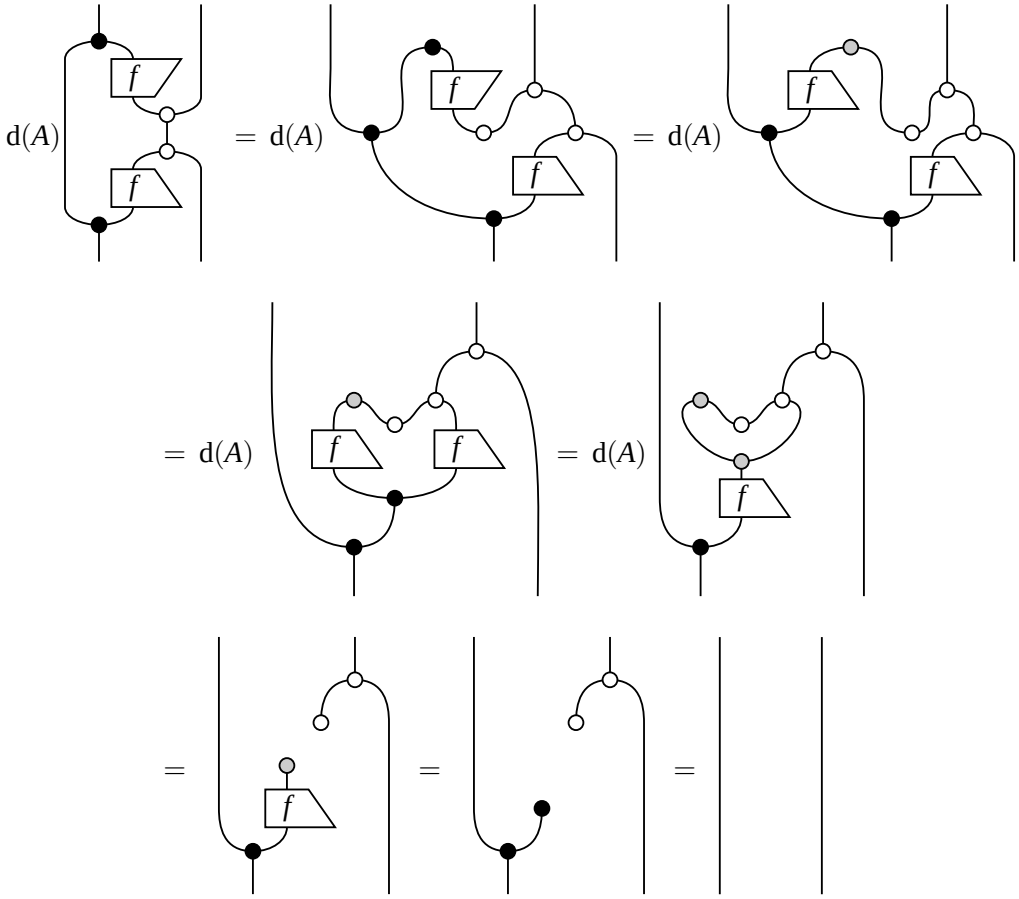
a self-conjugate comonoid homomorphism $f : (A, \curlyvee, \bullet) \to (B, \curlyvee, \circ)$, the *oracle* is defined to be the following endomorphism of $A \otimes B$:



(16)

Theorem 11. *Oracles are unitary.*

Proof. To demonstrate that the oracle (16) is unitary, we must compose it with its adjoint on both sides and show that we get the identity in each case. In one case, we obtain the following, making use of the Frobenius laws, self-conjugacy of f, associativity and coassociativity, the fact that f preserves comultiplication, the complementarity condition, the fact that f preserves the counit, and the unit and counit laws:



There is a similar argument that the other composite also gives the identity. □

3 Identifying group homomorphisms into abelian groups

3.1 Introduction

In this Section we construct a new deterministic quantum algorithm to identify group homomorphisms.

Definition 12 (Group homomorphism identification problem)**.** Given finite groups G and A where A is abelian, and a blackbox function $f : G \to A$ that is promised to be a group homomorphism, identify the homomorphism f.

We will define a quantum algorithm that solves the group homomorphism identification problem with a number of queries equal to the number of simple factors of the abelian group A.

For comparison, we can consider the obvious classical algorithm for this problem.

Lemma 13. *Given finite groups G and A, where A is abelian and G has a generating set of order m, and a blackbox function $f : G \to A$ that is promised to be a group homomorphism, a classical algorithm can determine f with m oracle queries.*

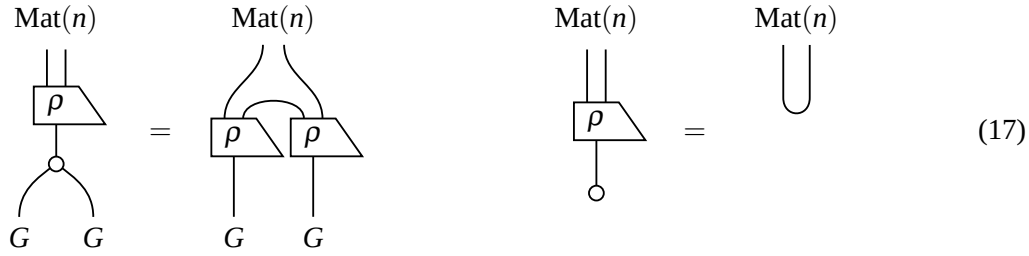
Proof. Once we have evaluated f classically on the generating set of G, we have fully characterized f. □

We are unable to prove optimality in either the quantum or classical case. However, we note that the query complexities of these quantum and classical algorithms depend of different and unrelated parameters of the problem. Instances where the order of the generating set of G is larger than the number of factors in the target group A will demonstrate a quantum advantage.

In the simpler case where G is an abelian group this quantum algorithm was previously described by Høyer [11], though his algebraic presentation differs significantly from ours. Høyer also notes that the algorithm by Bernstein and Vazirani in [3] is an instance of the abelian group identification problem where $G = \mathbb{Z}_n^n$ and $A = \mathbb{Z}_2$. Independently, Cleve et. al. [7] also presented an algorithm for the abelian case where $G = \mathbb{Z}_2^n$ and $A = \mathbb{Z}_2^m$.

We will proceed using the abstract structure defined earlier, but will now work in the dagger-symmetric monoidal category **FHilb**. Any choice of orthonormal basis for an object A in **FHilb** endows it with a dagger-Frobenius algebra $(A, \curvearrowleft, \bullet)$, whose copying map $d : A \to A \otimes A$ is defined as the linear extension of $d(|i\rangle) = |i\rangle \otimes |i\rangle$. Any finite group G induces a different dagger-Frobenius algebra on an object $A = \mathbb{C}[G]$, the Hilbert space with orthonormal basis given by the elements G, with multiplication given by linear extension of the group multiplication; we represent this structure as $(A, \curvearrowleft, \circ)$. These two Frobenius algebras are complementary.

In the case that G is finite, its representations can be characterized as the homomorphisms $G \xrightarrow{\rho} \mathrm{Mat}(n)$. The homomorphism conditions take the following form [13, Section A.7]:

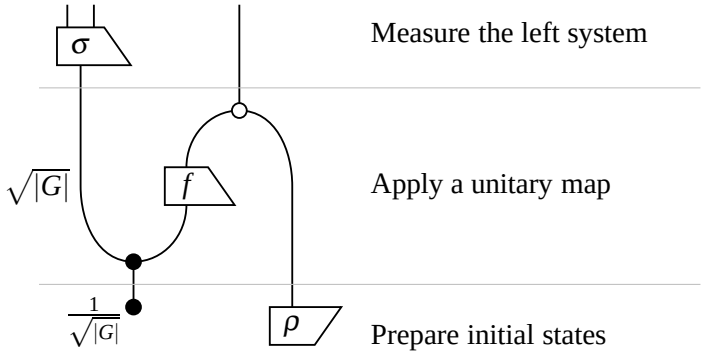


(17)

These will be essential for our proofs below.

3.2 The algorithm

The structure of the quantum algorithm that solves the group homomorphism identification problem is given by the topological diagram (18) below. Here $\sigma : G \to \mathbb{C}$ is a normalized irreducible representation of G, representing the result of the measurement, and $\rho : A \to \mathbb{C}$ is a normalized irreducible representation of A. The representation ρ is one-dimensional as A is an abelian group. Physically, we are able to produce the input state ρ efficiently, using $O(\log n)$ time steps, via the quantum Fourier transform for any finite abelian group [6]. The measurement result σ arises from a measurement in the Fourier basis, which can, by a similar procedure for any finite group [5], also be implemented efficiently.



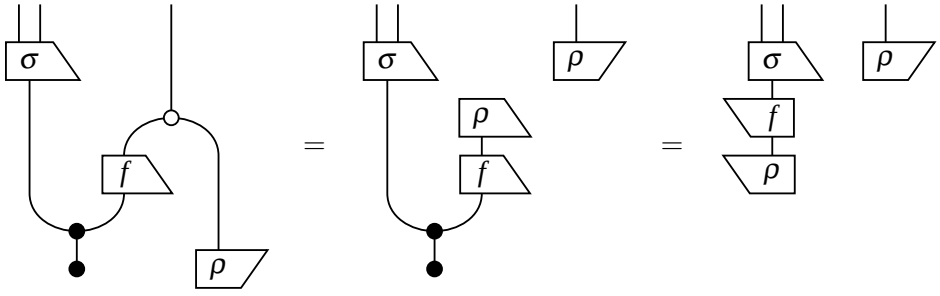
(18)

We can compare the structure of this algorithm to that of the standard quantum algorithm for the hidden subgroup problem. There, the second system is prepared in a state given by the identity element of the group, corresponding to a uniform linear combination of the irreducible representations. A later measurement of this second system—which is not a part of the standard hidden subgroup algorithm, but can be done without changing the result of the procedure—would collapse this combination to a classical mixture of these representations. The hidden subgroup algorithm therefore contains an amount of classical nondeterminism in its initial setup. In principle removing this, and selecting the input representation strategically, can only improve performance, and we take advantage of this here.

We analyze the effect of our new algorithm as follows.

Lemma 14. *The algorithm defined by* (18) *gives output σ with probability given by the square norm of $\sigma \circ f^* \circ \rho^*$.*

Proof. Using that ρ is a group homomorphism and simple diagrammatic rewrites defined in [13, Section A.9], we show the following, making use of the fact that representations are copyable points for group multiplication:



(19)

The left hand system is thus in the state $\sigma \circ f^* \circ \rho^*$, and using the Born rule, the squared norm of this state gives the probability of this experimental outcome. □

Lemma 15. *The composite $\rho \circ f$ is an irreducible representation of G.*

Proof. The map f is a homomorphism, so $\rho \circ f : G \to \mathbb{C}$ is a one-dimensional representation of G. All one-dimensional representations are irreducible, so $\rho \circ f$ is an irreducible representation. □

Lemma 16. *One-dimensional representations are equivalent only if they are equal.*

Proof. Let $\rho_1, \rho_2 : G \to \mathbb{C}$ be irreducible representations of G. If they are isomorphic, then there exists a linear map $\mathscr{L} : \mathbb{C} \to \mathbb{C}$, i.e. some complex number, such that $\forall g \in G$

$$\mathscr{L}\rho_1(g) = \rho_2(g)\mathscr{L}.$$

Hence we see that $\forall g \in G$, $\rho_1(g) = \rho_2(g)$. □

Theorem 17 (Structure theorem for finite abelian groups)**.** *Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.*

Proof. See [1, Theorem 6.4] for a proof of this standard result. □

Theorem 18. *For a finite group G and cyclic group of prime power order $\mathbb{Z}_{p^n}$, the algorithm* (18) *identifies a group homomorphism $f : G \to \mathbb{Z}_{p^n}$ in a single query.*

Proof. Choose the input representation ρ to be the fundamental representation of $\mathbb{Z}_{p^n}$. This representation is faithful. This means exactly that

$$\rho \circ f = \rho \circ f' \qquad \Leftrightarrow \qquad f = f'.$$

Thus $\rho \circ f$ and $\rho \circ f'$ are different irreducible representations if and only if f and f' are different group homomorphisms. The single measurement on the state $(\rho \circ f)^*$ is performed by the algorithm in the representation basis of G, allowing us to determine $\rho \circ f$ up to isomorphism. Due to Lemma 16 we know that each equivalence class contains only one representative, and thus we can determine f with a single query. □

Theorem 19. *For any two finite groups G and A, where A is abelian with n simple factors, the quantum algorithm* (18) *can identify a group homomorphism $f : G \to A$ with n oracle queries.*

Proof. We prove the result by induction.

Base case. When $A = \mathbb{Z}_{p^n}$ is simple, then by Theorem 18 we can identify the homomorphism with a single query.

Inductive step. If A is not simple, then we must have $A = H_1 \times H_2$ by Theorem 17, where the following hold:

1. The product $\times$ is the direct product whose projectors (p_1, p_2) are homomorphisms.
2. H_1 and H_2 are groups with n_1 and n_2 factors respectively such that the theorem holds, i.e. homomorphisms of the type $f_1 : G \to H_1$ and $f_2 : G \to H_2$ can be identified in n_1 and n_2 queries respectively.

Since $p_1 \circ f$ and $p_2 \circ f$ are homomorphisms, we can run subroutines of the algorithm to determine them. Hence we recover f as

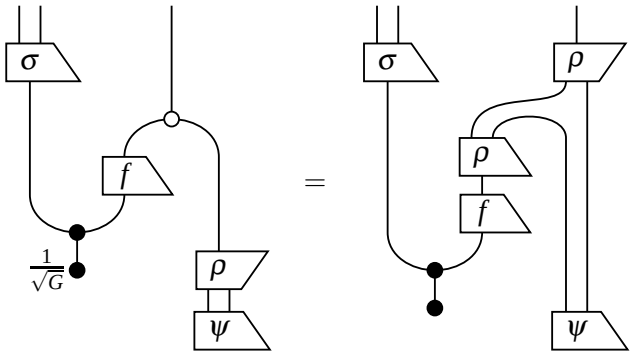
$$f(x) = ((p_1 \circ f)(x), (p_2 \circ f)(x)).$$

The first subroutine will require n_1 queries and the second will require n_2 queries, so the total number of queries will be $n_1 + n_2$, which is the number of factors of $H_1 \times H_2$. □

3.3 Extension to the non-abelian case

We now consider the more general case where the target group A is non-abelian. We do not know how to extend the algorithm described above to this case. Nevertheless, it is instructive to analyze this scenario in our graphical approach.

Irreducible representations of a non-abelian group A are not necessarily one dimensional, though we are still able to compute them via the Fourier transform efficiently [5]. In this case the algorithm has the following structure, where ψ represents the initial state of the right-hand system in the representation space:



(20)

We notice two additional features in this case. First, it is clear that the left and right systems are no longer in a product state at the end of the protocol, as they were in the final diagram of (19). Second, we now have an additional choice when preparing the input representation ρ; in order to construct a state from a representation ρ we also must choose the state ψ.

While this provides a clear description of the algorithm in this more general setting, it is not clear that it would identify homomorphisms into non-abelian groups. Complications include the lack of a structure theorem that satisfies the conditions for Theorem 19, and that Lemma 15 no longer applies. In this setting it may be useful to make the problem easier by restricting to the identification of homomorphisms up to *natural isomorphism*, i.e. where two homomorphisms $f_1, f_2 : G \to H$ are considered equivalent when there exists some $\eta \in H$ such that, for all $g \in G$, we have $\eta f_1(g) \eta^{-1} = f_2(g)$.

4 Application to signal-flow calculus

4.1 Introduction

Signal-flow diagrams are a notation in electrical engineering that describe the flow of information in electrical circuits, including rich phenomena such as feedback. Various authors [2, 4, 10] have have developed a categorical approach to modelling signal-flow diagrams, based on a category of linear relations on vector spaces over a field k. We show in this Section that unitary oracles exist in their setup, in the sense of our Definition 10, and discuss the consequences of this.

We begin with a brief introduction to the theory, following the terminology of [2].

Definition 20. The category $\mathbf{FinRel}_k$ of *linear relations* is defined in the following way, for any field k:

- **Objects** are finite dimensional k-vector spaces
- A **morphism** $f : V \rightsquigarrow W$ is a *linear relation*, defined as a subspace $S_f \hookrightarrow V \oplus W$
- **Composition** of linear relations $f : U \rightsquigarrow V$ and $g : V \rightsquigarrow W$ is defined as the following subspace of $U \oplus W$:

$$\{(u,w) | \exists v \in V \text{ with } (u,v) \in S_f \text{ and } (v,w) \in S_g\} \tag{21}$$

  It can be verified that this defines a linear subspace of $U \oplus W$.

Note that a linear relation is in particular an ordinary relation, and that composition of linear relations is the same as for ordinary relations. The category $\mathbf{FinRel}_k$ can be given a monoidal structure in a natural way, using the direct sum of vector spaces.

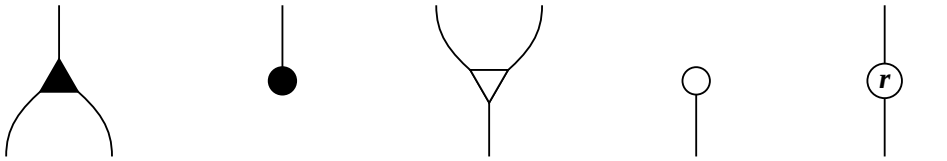
For every linear relation, we can define a converse as follows.

Definition 21. Given a linear relation $f : U \rightsquigarrow V$ defined as the subspace $S_f \hookrightarrow U \oplus V$, its *converse* is the linear relation $f^\dagger : V \rightsquigarrow U$ defined as the subspace $S_f \hookrightarrow U \oplus V \xrightarrow{\text{swap}} V \oplus U$.

This makes $\mathbf{FinRel}_k$ into a monoidal dagger-category. Following the usual convention [12], we depict the dagger of a linear relation as the original morphism flipped about a horizontal axis.

Certain canonical linear relations play an important role in the theory. We define them here, along with the graphical symbol we will use to denote them.

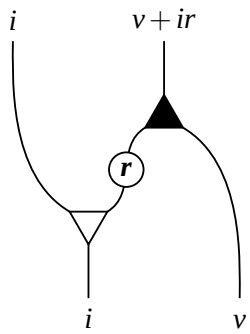
Definition 22. The *addition*, *zero*, *copying*, *deletion* and *multiplier* linear relations are defined as follows, where the definitions in the last line are valid for all $a, b \in k$, and where the multiplier relation takes a parameter given by some $r \in k$:



Addition	Zero	Copying	Deletion	Multiplier
$\blacktriangle : k \oplus k \rightsquigarrow k$	$\bullet : \{0\} \rightsquigarrow k$	$\nabla : k \rightsquigarrow k \oplus k$	$\circ : k \rightsquigarrow \{0\}$	$\boldsymbol{r} : k \rightsquigarrow k$
$(a,b,a+b) \in \blacktriangle$	$(0,0) \in \bullet$	$(a,a,a) \in \nabla$	$(a,0) \in \circ$	$(a,ra) \in \boldsymbol{r}$

(22)

They use their theory to model resistors in electrical circuits, using the following network:



(23)

The left-hand wire represents the current variable, and the right-hand wire represents the voltage variable. The initial current-voltage pair (i,v) is mapped to the output current-voltage pair $(i,v+ir)$. This respects the usual law for resistors in electrical circuits, whereby if δv is the change in voltage over a resistor, i is the current through the resistor, and the value of the resistance is r, then $\delta v = ir$.

It has been recognized in [2] that the linear relations given in Definition 22 satisfy many interesting relationships, which we summarize here without proof:

Lemma 23. *In* $\mathbf{FinRel}_k$*, the following relationships hold between the addition, zero, copying, deletion and multiplier linear relations:*

1. *Addition and zero together form a commutative monoid.*
2. *Copying and deletion together form a commutative comonoid.*
3. *This monoid and comonoid together form a bialgebra.*
4. *The multiplier relation is a monoid homomorphism for addition, and a comonoid homomorphism for copying.*

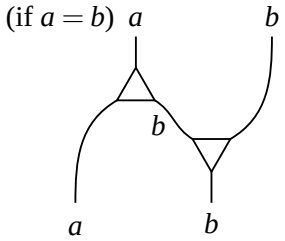
4.2 Complementary dagger-Frobenius structure

In this section we prove new results about the structures introduced in Section 4.1. We begin by establishing the existence of dagger-Frobenius properties of the addition and copying operations.

Lemma 24. *In* $\mathbf{FinRel}_k$*, the addition and copying linear relations separately form commutative dagger-Frobenius algebras.*

Proof. That addition and zero forms a commutative monoid, and copying and deletion forms a commutative comonoid, is established in Lemma 23. It remains to demonstrate that the dagger-Frobenius conditions hold for each of these structures.

We first evaluate the action of the following composite linear relation, which is one side of the dagger-Frobenius condition for the copying linear relation:

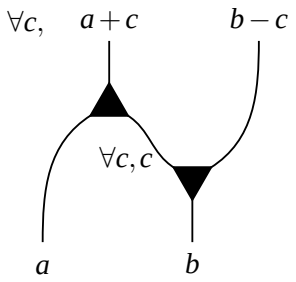


(24)

We see that this composite relation can be defined as $\forall a,(a,a)$  (a,a), and similarly it can be shown that $\forall a,(a,a)$  (a,a). Hence we have demonstrated the dagger-Frobenius condition = .

For the addition linear relation, we calculate the left side of the dagger-Frobenius condition as

follows:



(25)

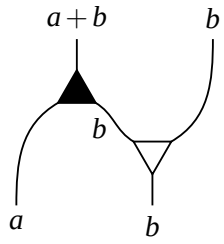
We can write this action succinctly as $\forall c,(a,b)$  $(a+c,b-c)$. Similarly, the other composite can be shown to have action $\forall c,(a,b)$  $(a-c,b+c)$. Making the substitution $c' := -c$, we can rewrite this second definition as $\forall c',(a,b)$ $(a+c',b-c')$. This demonstrates that $=$ as linear relations, verifying the dagger-Frobenius condition for the addition linear relation. □

Furthermore, these Frobenius algebras interact as complementary structures.

Lemma 25. *In* $\mathbf{FinRel}_k$*, the addition and copying linear relations form complementary dagger-Frobenius algebras.*

Proof. We have already established the Frobenius properties in Lemma 24. It remains to demonstrate the complementarity condition.

We evaluate the action of the following composite relation:



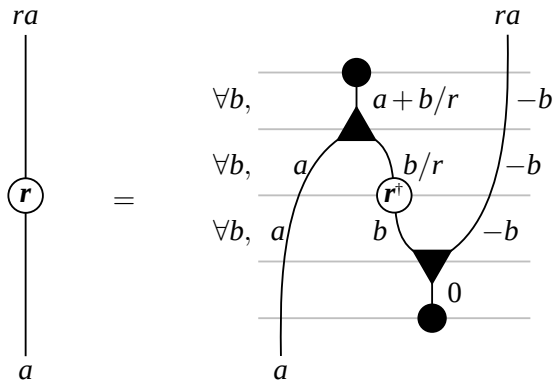
(26)

Writing K for this linear relation, we see that K is given by $\forall a,b \in k,(a,b)K(a+b,b)$. By Definition 21 of the converse relation, we see that $K^\dagger$ is defined as $\forall a,b \in k,(a+b,b)K^\dagger(a,b)$, or equivalently $\forall a,b \in k,(a,b)K^\dagger(a-b,b)$. Since K is single-valued and total, it is clear that K and $K^\dagger$ are inverse, as can be shown by explicit calculation. By Theorem 9, it follows that addition and copying are complementary. □

The final property that we establish is that multipliers are self-conjugate.

Lemma 26. *In* $\mathbf{FinRel}_k$*, a multiplier* $\boldsymbol{r} : k \rightsquigarrow k$ *is a self-conjugate morphism.*

Proof. We must verify that $\boldsymbol{r}$ is equal to the transpose of its dagger:



(27)

On the right-hand side we see that a is related to $-b$, with the constraint that $a + b/r = 0$, i.e. that $-b = ra$. This is equal as a linear relation to that of $\boldsymbol{r}$ itself, given on the left-hand side. This establishes the result. □

Given these results, we are motivated to make the following definitions which generalize the motivating example of the theory of signal-flow diagrams in $\mathbf{FinRel}_k$.

Definition 27. In a symmetric monoidal dagger-category, a *signal-flow structure* is an object A equipped with a pair of commutative dagger-Frobenius algebras, which interact as a bialgebra. A *multiplier* for this signal-flow structure is a self-conjugate morphism $\boldsymbol{r} : A \to A$ which is a monoid and comonoid homomorphism for both structures.

Definition 28. Given a signal-flow structure equipped with a multiplier $\boldsymbol{r}$, the *resistor* associated to $\boldsymbol{r}$ is the composite given by diagram (23).

We then apply our earlier result to show that resistors are always unitary.

Corollary 29. *Given a signal-flow structure equipped with a multiplier, its resistor is unitary.*

Proof. An immediate application of Theorem 11. □

The appearance of this unitary structure in both quantum algorithm and the signal-flow calculus highlights the general role that this abstract structure can play in different process theories.

References

[1] Michael Artin (1991): *Algebra*. Prentice Hall.

[2] John Baez & Jason Erbele (2014): *Categories in Control*. arXiv:1405.6881.

[3] Ethan Bernstein & Umesh Vazirani (1997): *Quantum Complexity Theory*. *SIAM J. on Computing* 26(5), pp. 1411–1473, doi:10.1145/167088.167097.

[4] Filippo Bonchi, Pawel Sobocinski & Fabio Zanasi (2014): *Interacting Hopf Algebras*. arXiv:1403:7048.

[5] Andrew M. Childs & Wim van Dam (2010): *Quantum Algorithms for Algebraic Problems*. *Reviews of Modern Physics* 82, pp. 1–52, doi:10.1103/RevModPhys.82.1. arXiv:0812.0380.

[6] R. Cleve & J. Watrous (2000): *Fast Parallel Circuits for the Quantum Fourier Transform*. *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, pp. 526–536, doi:10.1109/SFCS.2000.892140. arXiv:quant-ph/0006004.

[7] Richard Cleve, Artur Ekert, Chiara Macchiavello & Michele Mosca (1998): *Quantum Algorithms Revisited*. *Proc. R. Soc. Lond.* 454(1969), pp. 339–354, doi:10.1098/rspa.1998.0164. arXiv:quant-ph/9708016.

[8] Bob Coecke & Ross Duncan (2011): *Interacting Quantum Observables: Categorical Algebra and Diagrammatics*. *New Journal of Physics* 13, doi:10.1088/1367-2630/13/4/043016. arXiv:0906.4725.

[9] Bob Coecke, Dusko Pavlovic & Jamie Vicary (2008): *A New Description of Orthogonal Bases*. *Mathematical Structures in Computer Science* 23(3), doi:10.1017/S0960129512000047. arXiv:0810.0812.

[10] Brendan Fong (2013): *A Compositional Approach to Control Theory*. Transfer of status report. Available at http://math.ucr.edu/home/baez/networks_oxford/.

[11] Peter Høyer (1999): *Conjugated Operators in Quantum Algorithms*. *Physical Review A* 59(5), pp. 3280–3289, doi:10.1103/PhysRevA.59.3280.

[12] Peter Selinger (2011): *A Survey of Graphical Languages for Monoidal Categories*. *Springer Lecture Notes in Physics* (813), pp. 289–355, doi:10.1007/978-3-642-12821-9_4. arXiv:0908.3347.

[13] Jamie Vicary (2013): *Topological Structure of Quantum Algorithms*. *Proceedings of 28th Annual ACM/IEEE Symposium on Logic in Computer Science*, pp. 93–102, doi:10.1109/LICS.2013.14. arXiv:1209.3917.