Abstract structure of unitary oracles for quantum algorithms

William Zeng[1] Jamie Vicary[2]

[1]Department of Computer Science
University of Oxford

[2]Centre for Quantum Technologies, University of Singapore
and Department of Computer Science, University of Oxford

Quantum Physics and Logic, 2014

Unitary Oracles

- Oracles are common structures in algorithms. They are blackboxes with unknown internal structure.

Unitary Oracles

- Oracles are common structures in algorithms. They are blackboxes with unknown internal structure.
- Most known quantum algorithms are constructed using quantum oracles, the Deutsch-Josza algorithm, Shor's algorithm, Grover's algorithm...

Unitary Oracles

- Oracles are common structures in algorithms. They are blackboxes with unknown internal structure.
- Most known quantum algorithms are constructed using quantum oracles, the Deutsch-Josza algorithm, Shor's algorithm, Grover's algorithm...
- Physical realizations of oracles place conditions on their "unknown" structure. (Unitarity in the quantum case)

Unitary Oracles

- Oracles are common structures in algorithms. They are blackboxes with unknown internal structure.
- Most known quantum algorithms are constructed using quantum oracles, the Deutsch-Josza algorithm, Shor's algorithm, Grover's algorithm...
- Physical realizations of oracles place conditions on their "unknown" structure. (Unitarity in the quantum case)

Main questions:

Unitary Oracles

- Oracles are common structures in algorithms. They are blackboxes with unknown internal structure.
- Most known quantum algorithms are constructed using quantum oracles, the Deutsch-Josza algorithm, Shor's algorithm, Grover's algorithm...
- Physical realizations of oracles place conditions on their "unknown" structure. (Unitarity in the quantum case)

Main questions:

- What is the abstract structure of these oracles?

Unitary Oracles

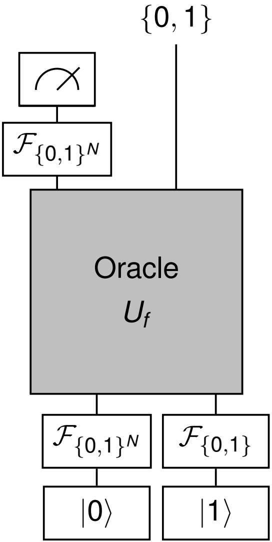
- Oracles are common structures in algorithms. They are blackboxes with unknown internal structure.
- Most known quantum algorithms are constructed using quantum oracles, the Deutsch-Josza algorithm, Shor's algorithm, Grover's algorithm...
- Physical realizations of oracles place conditions on their "unknown" structure. (Unitarity in the quantum case)

Main questions:

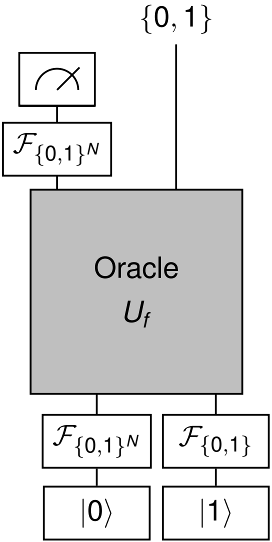
- What is the abstract structure of these oracles?
- Can we take advantage of this abstract setting to gain new insights?

Unitary Oracles

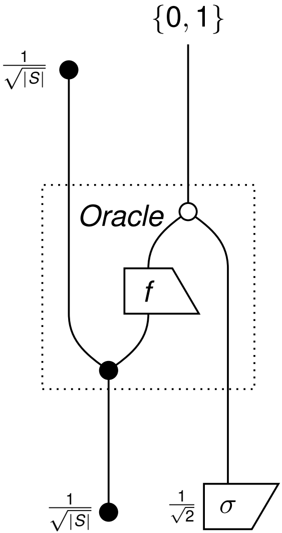
The traditional Deutsch-Joza circuit is:



Unitary Oracles

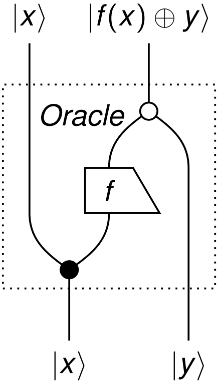


Here is its abstract structure:



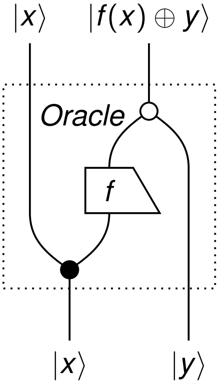
Unitary Oracles

This is the oracle's internal structure:



Unitary Oracles

This is the oracle's internal structure:

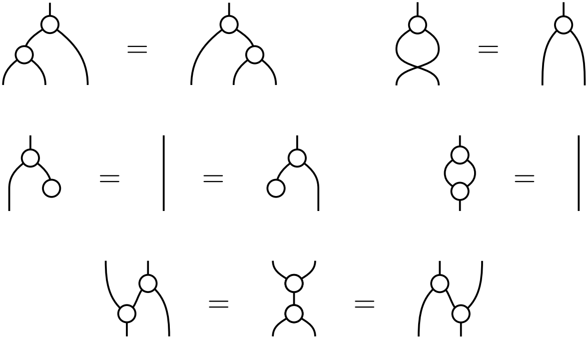


Theorem

Oracles with this abstract structure are unitary in general.

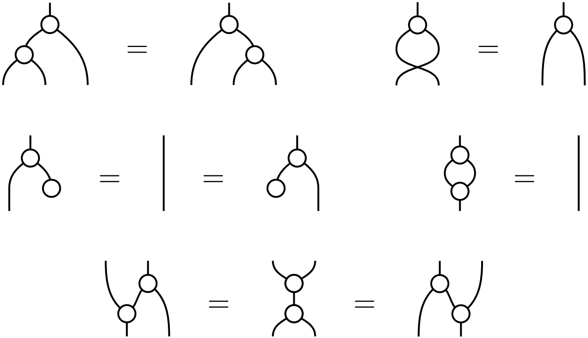
Categorical Quantum Information

Definition: A special †-Frobenius algebra obeys:



Categorical Quantum Information

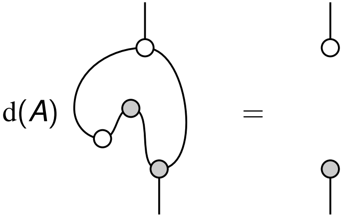
Definition: A special †-Frobenius algebra obeys:



This represents the abstract structure of an *observable*.

Complementary observables

Definition [Coecke & Duncan]: Two †-Frobenius algebras on the same object are complementary when:



Complementary observables

Complementary observables in **FHilb** come from finite abelian groups

- Copying

 $:: |g\rangle \mapsto |g\rangle \otimes |g\rangle$

 $:: |g\rangle \mapsto 1$

- Group multiplication

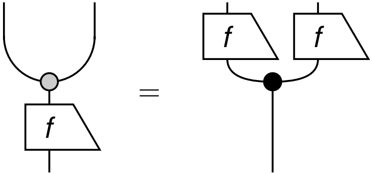
 $:: |g_1\rangle \otimes |g_2\rangle \mapsto \frac{1}{\sqrt{D}}|g_1 \oplus g_2\rangle$

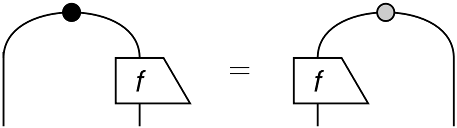
 $:: |1\rangle \mapsto \sqrt{D}|0\rangle$

Classical Maps

Definition:

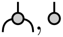
A classical map $f : (A, \text{black multiplication}, \text{black unit}) \to (B, \text{grey multiplication}, \text{grey unit})$ obeys:

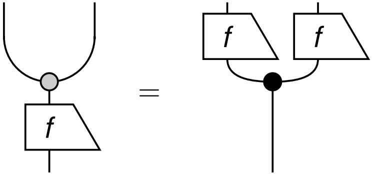


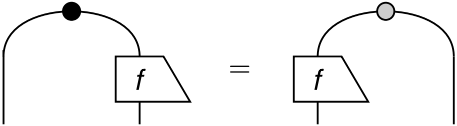


Classical Maps

Definition:

A classical map $f : (A,$  $) \to (B,$  $)$ obeys:





These are self-conjugate comonoid homomorphisms.

Unitarity Theorem

- Three †-Frobenius algebras, (◉ , ○, ●)

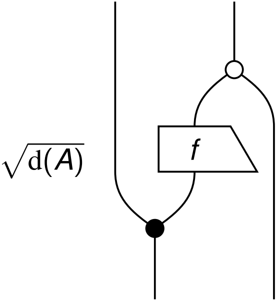
Unitarity Theorem

- Three †-Frobenius algebras, (● , ○, ●)
- A pair are complementary (● and ○)

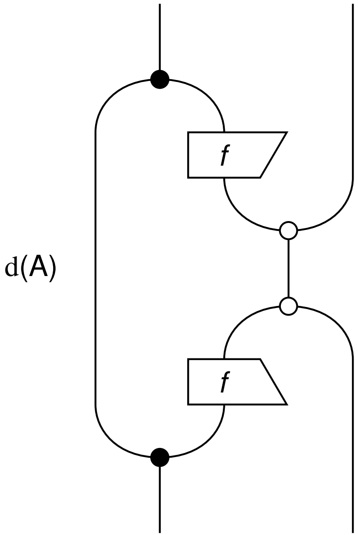
Unitarity Theorem

- Three †-Frobenius algebras, (◉ , ○, ●)
- A pair are complementary (◉ and ○)
- A classical map $f : (A, ⅄●, ●) \to (B, ⅄◉, ◉)$

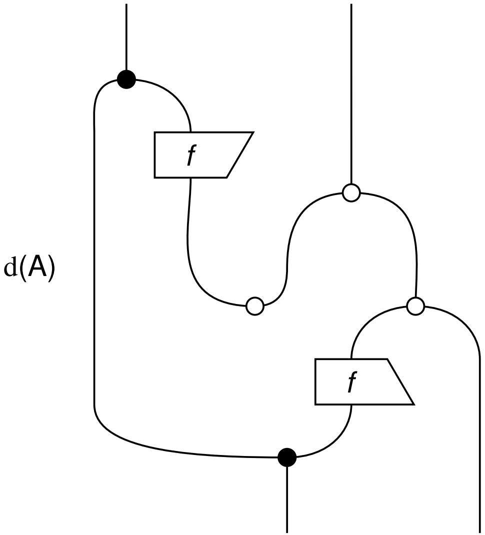
Produce the *unitary* morphism:



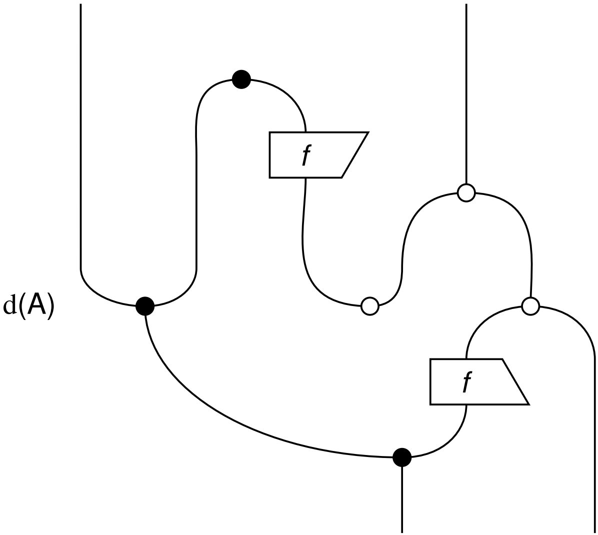
Abstract proof of unitarity



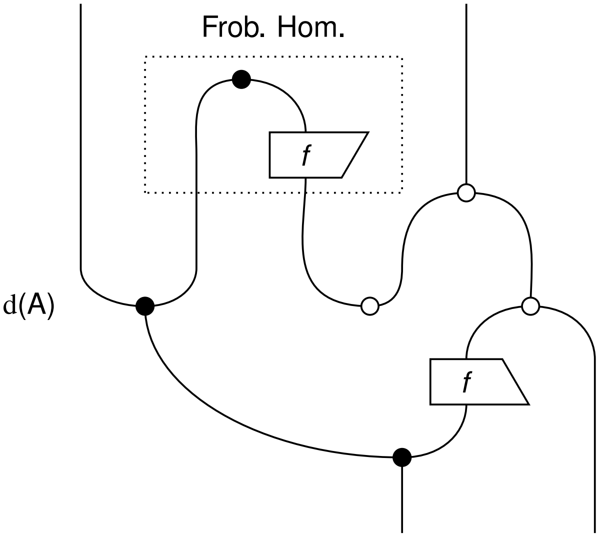
Abstract proof of unitarity



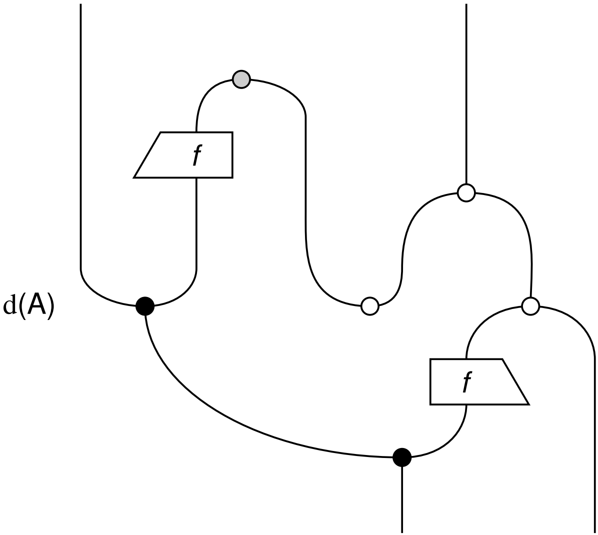
Abstract proof of unitarity



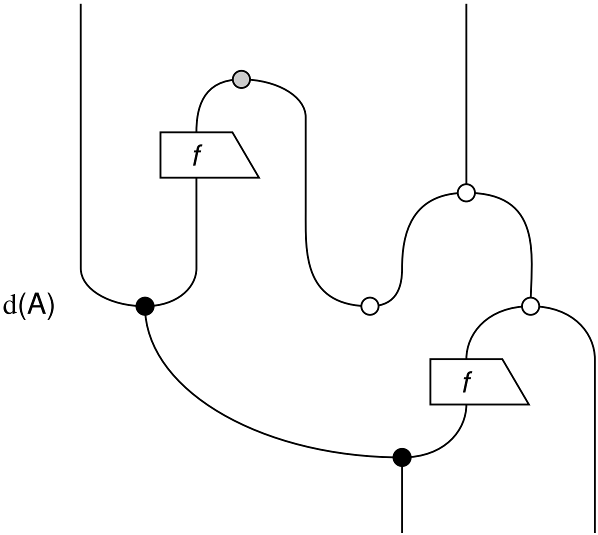
Abstract proof of unitarity



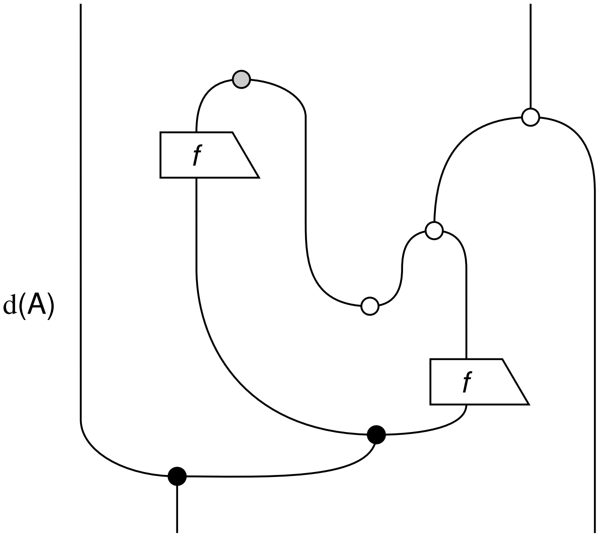
Abstract proof of unitarity



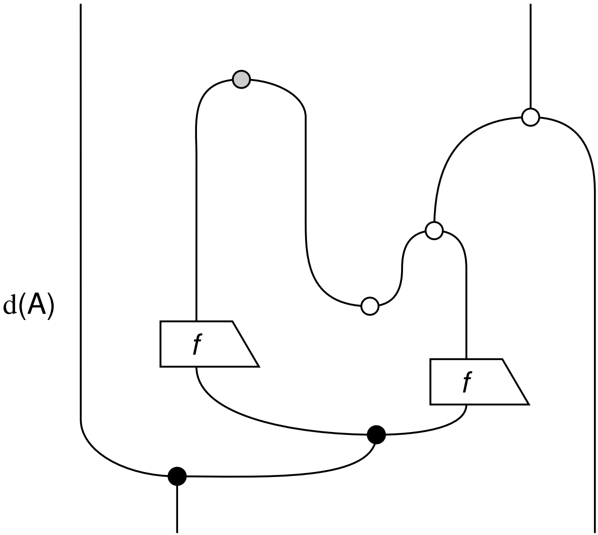
Abstract proof of unitarity



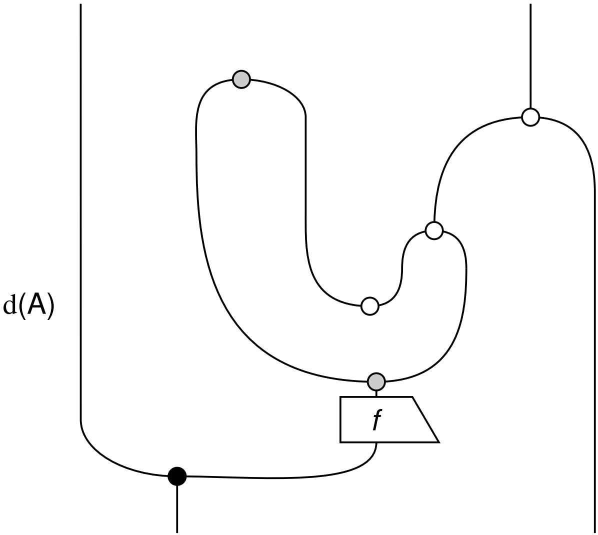
Abstract proof of unitarity



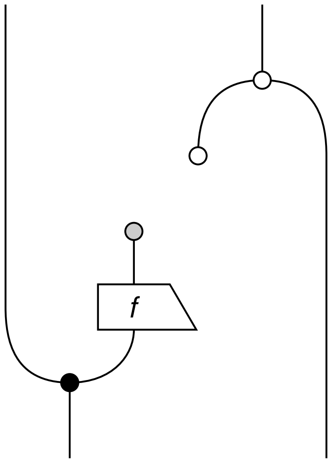
Abstract proof of unitarity



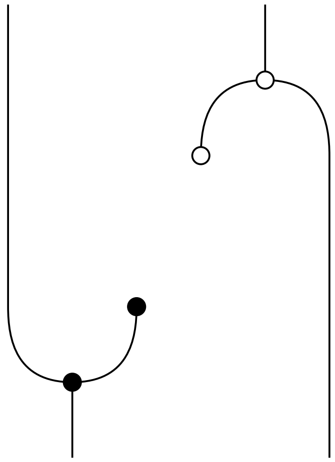
Abstract proof of unitarity



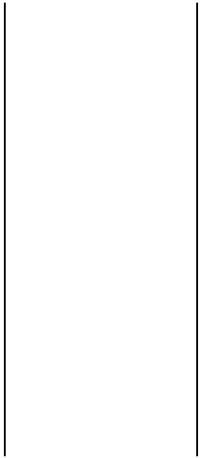
Abstract proof of unitarity



Abstract proof of unitarity



Abstract proof of unitarity



Unitary Oracles

- We have defined (diagrammatically) an abstract structure required to make oracles physical.

Unitary Oracles

- We have defined (diagrammatically) an abstract structure required to make oracles physical.
- This lifts the property of unitarity for quantum oracles to the more abstract setting of dagger monoidal categories.

Unitary Oracles

- We have defined (diagrammatically) an abstract structure required to make oracles physical.
- This lifts the property of unitarity for quantum oracles to the more abstract setting of dagger monoidal categories.
- Can we take advantage of this abstract setting to gain new insights?

Unitary Oracles

- We have defined (diagrammatically) an abstract structure required to make oracles physical.
- This lifts the property of unitarity for quantum oracles to the more abstract setting of dagger monoidal categories.
- Can we take advantage of this abstract setting to gain new insights? Yes.
  - To develop a new group theoretic quantum algorithm
  - To apply result in signal-flow calculus

The group homomorphism identification problem

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

The group homomorphism identification problem

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

- Group representations are $\rho : G \to \mathrm{Mat}(n)$

The group homomorphism identification problem

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

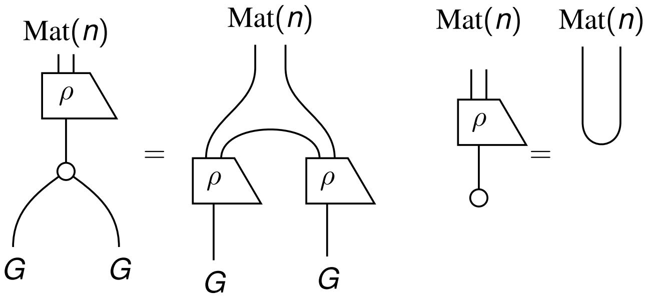
- Group representations are $\rho : G \to \mathrm{Mat}(n)$

- Group Representations as measurements: projections onto a subspace

The group homomorphism identification problem

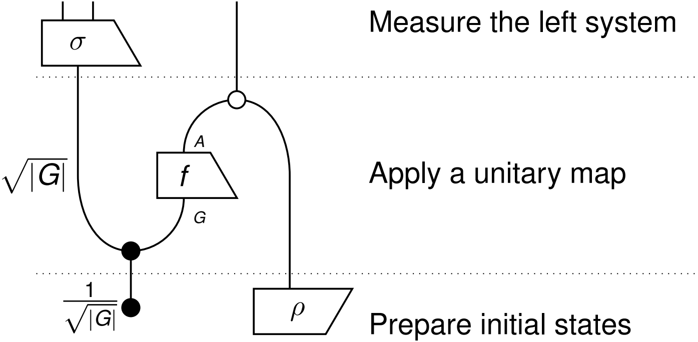
- **Definition. (Group homomorphism identification problem)** Given finite groups G and A where A is abelian, and a blackbox function $f : G \to A$ promised to be a group homomorphism, identify f.

- Graphical rules for group representations:

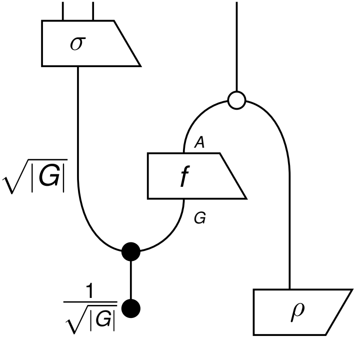


The group homomorphism identification algorithm

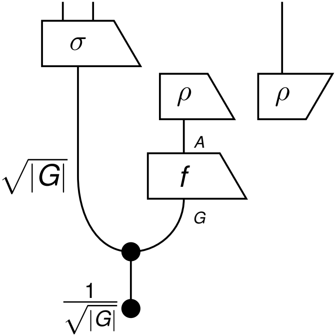
Case: Let A be a cyclic group $\mathbb{Z}_n$.



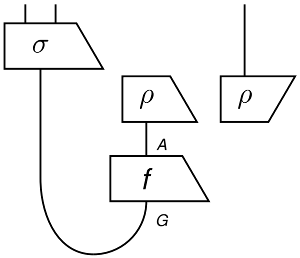
The group homomorphism identification algorithm



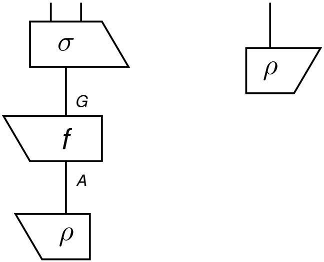
The group homomorphism identification algorithm



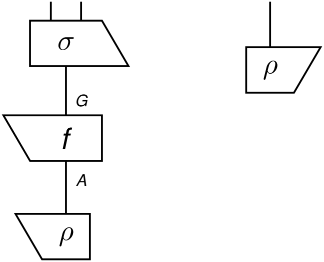
The group homomorphism identification algorithm



The group homomorphism identification algorithm

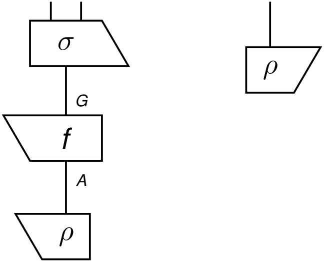


The group homomorphism identification algorithm



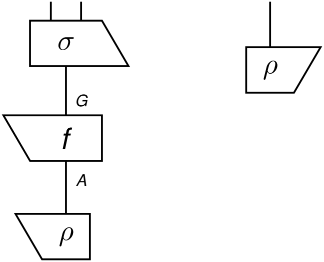
- $\rho \circ f$ is an irreducible representation of A.

The group homomorphism identification algorithm



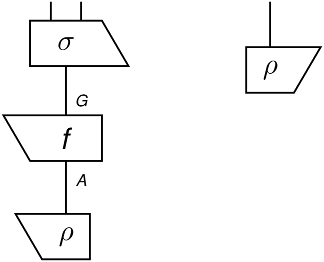
- $\rho \circ f$ is an irreducible representation of A.
- Choose ρ to be a faithful representation of A.

The group homomorphism identification algorithm



- $\rho \circ f$ is an irreducible representation of A.
- Choose ρ to be a faithful representation of A.
- Then measuring $\rho \circ f$ identifies f (up to isomorphism)

The group homomorphism identification algorithm



- $\rho \circ f$ is an irreducible representation of A.
- Choose ρ to be a faithful representation of A.
- Then measuring $\rho \circ f$ identifies f (up to isomorphism)
- One-dimensional representations are isomorphic only if they are equal.

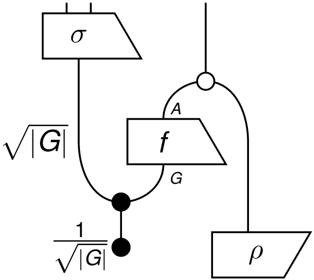
The group homomorphism identification algorithm

Homomorphism $f : G \to A$

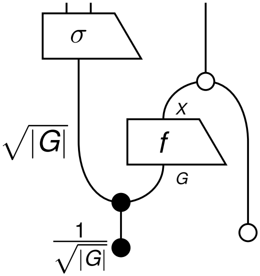
- We generalize with proof by induction via the Structure Theorem. $A = Z_{p_1} \oplus ... \oplus Z_{p_k}$
- Can identify the group homomorphism in k oracle queries.
- The naive classical solution requires a number of queries equal to the number of factors of G rather than A.

Comparison to the hidden subgroup algorithm

Group ID

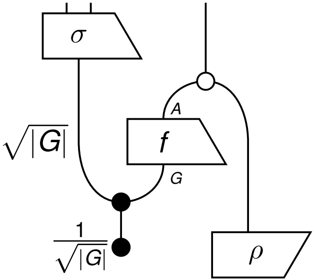


Hidden Subgroup

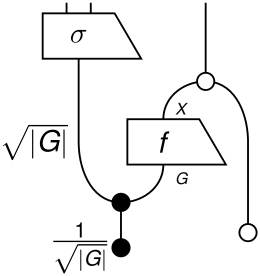


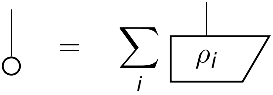
Comparison to the hidden subgroup algorithm

Group ID



Hidden Subgroup





FinRel$_k$

[Baez, Erlebe, Fong 2014]

Definition

The category **FinRel**$_k$ of *linear relations* is defined in the following way, for any field k:

- **Objects** are finite dimensional k-vector spaces

$\mathbf{FinRel}_k$

[Baez, Erlebe, Fong 2014]

Definition

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** $f : V \to W$ is a *linear relation*, defined as a subspace $S_f \hookrightarrow V \oplus W$

$\mathbf{FinRel}_k$

[Baez, Erlebe, Fong 2014]

Definition

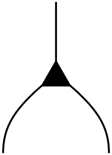
The category $\mathbf{FinRel}_k$ of *linear relations* is defined in the following way, for any field k:

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

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

  This defines a linear subspace of $U \oplus W$.

The signal-flow calculus $\mathbf{FinRel}_k$



Addition

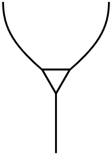
$\blacktriangle : k \oplus k \to k$

$(a, b, a+b) \in \blacktriangle$

Zero

$\bullet : \{0\} \to k$

$(0, 0) \in \bullet$



Copying

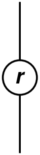
$\nabla : k \to k \oplus k$

$(a, a, a) \in \nabla$

Deletion

$\circ : k \to \{0\}$

$(a, 0) \in \circ$

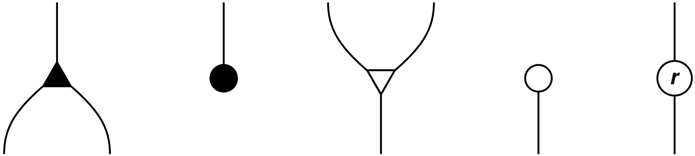


Multiplier

$\boldsymbol{r} : k \to k$

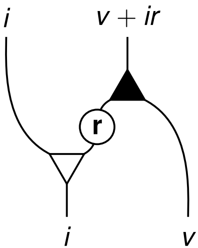
$(a, ra) \in \boldsymbol{r}$

The signal-flow calculus $\mathbf{FinRel}_k$



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

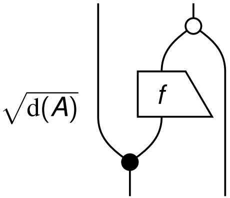
- Resistor



Conclusions (arxiv: 1406.1278)

- Theorem

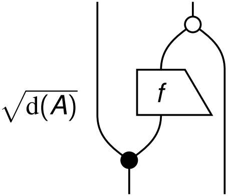
  A pair of complementary dagger-Frobenius algebras, equipped with a classical map onto one of the algebras, produce a unitary morphism:



Conclusions (arxiv: 1406.1278)

- Theorem

  A pair of complementary dagger-Frobenius algebras, equipped with a classical map onto one of the algebras, produce a unitary morphism:

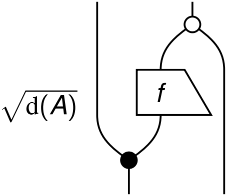


  - Abstract understanding of oracle in quantum computation

Conclusions (arxiv: 1406.1278)

- Theorem

  A pair of complementary dagger-Frobenius algebras, equipped with a classical map onto one of the algebras, produce a unitary morphism:

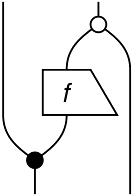
  

  - Abstract understanding of oracle in quantum computation
  - Apply this to develop a new algorithm for the deterministic identification of group homomorphisms into abelian groups.

Conclusions (arxiv: 1406.1278)

- Theorem

  A pair of complementary dagger-Frobenius algebras, equipped with a classical map onto one of the algebras, produce a unitary morphism:

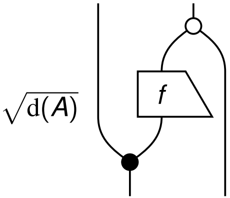
  $\sqrt{\mathrm{d}(A)}$ 

  - Abstract understanding of oracle in quantum computation
  - Apply this to develop a new algorithm for the deterministic identification of group homomorphisms into abelian groups.
  - Find the same structure in the theory of signal-flow networks.

Conclusions (arxiv: 1406.1278)

- Theorem

  A pair of complementary dagger-Frobenius algebras, equipped with a classical map onto one of the algebras, produce a unitary morphism:



  - Abstract understanding of oracle in quantum computation
  - Apply this to develop a new algorithm for the deterministic identification of group homomorphisms into abelian groups.
  - Find the same structure in the theory of signal-flow networks.
  - Big Idea: Symmetric monoidal categorical setting productively unifies process theories at an abstract level.

The Non-Abelian Case