Quantum algorithms in categorical quantum mechanics

William Zeng

Department of Computer Science
University of Oxford

10 years of CQM
October, 2014

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*
- **Open question** (Theoretical): What does this mean?

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*
- **Open question** (Theoretical): What does this mean?
  - What is the physical role of computational complexity?
  - What structures lead to speedups?

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*
- **Open question** (Theoretical): What does this mean?
  - What is the physical role of computational complexity?
  - What structures lead to speedups?
- **Open question** (Applied): What can we do with it?
  - How do we find useful quantum algorithms?

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*
- **Open question** (Theoretical): What does this mean?
  - What is the physical role of computational complexity?
  - What structures lead to speedups?
- **Open question** (Applied): What can we do with it?
  - How do we find useful quantum algorithms?

The CQM approach:

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*
- **Open question** (Theoretical): What does this mean?
  - What is the physical role of computational complexity?
  - What structures lead to speedups?
- **Open question** (Applied): What can we do with it?
  - How do we find useful quantum algorithms?

The CQM approach:

1. QM as an instance of general process theories in compact closed categories

Why quantum algorithms?

- Quantum algorithms as a change of perspective, i.e. *view physical structure as information processing*
- **Open question** (Theoretical): What does this mean?
  - What is the physical role of computational complexity?
  - What structures lead to speedups?
- **Open question** (Applied): What can we do with it?
  - How do we find useful quantum algorithms?

The CQM approach:

1. QM as an instance of general process theories in compact closed categories
2. Leverage the general setting and diagrammatic calculus to identify and exploit algorithmically useful structure

Overview

Quantum Algorithms: State of the Union

Blackbox algorithms in CQM: the old, the generalized, and the new

- Unitary Oracles
- Deutsch-Jozsa algorithm
- Hidden subgroup algorithms
- Group homomorphism identification algorithm
- Single-shot Grovers algorithm

Leveraging generality: other categories

Frontiers

- Quantum machine learning and connections to NLP

Quantum Algorithms: State of the Union

Many different techniques are used in practice:

Quantum Fourier transform

Hamilton simulation

Phase estimation

Quantum walks

Topological quantum algorithms

Adiabatic optimization

Amplitude estimation

etc.

Quantum Algorithms: State of the Union

- The quantum algorithm zoo (http://math.nist.gov/quantum/zoo/) lists some 42 different quantum algorithms
  - Only a handful show promise of exponential speedup
  - Three main categories: Algebraic/Number Theoretic, Approximation/Simulation, Oracular

Quantum Algorithms: State of the Union

- The quantum algorithm zoo (http://math.nist.gov/quantum/zoo/) lists some 42 different quantum algorithms
  - Only a handful show promise of exponential speedup
  - Three main categories: Algebraic/Number Theoretic, Approximation/Simulation, Oracular
- **Open question**: Is there a general theorem that tells us when we can hope for exponential speedups from quantum algorithms, and when we cannot? [Aaronson and Ambainis 2014]

Unitary Oracles

- Oracles are blackboxes with unknown internal structure.

Unitary Oracles

- Oracles 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 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 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

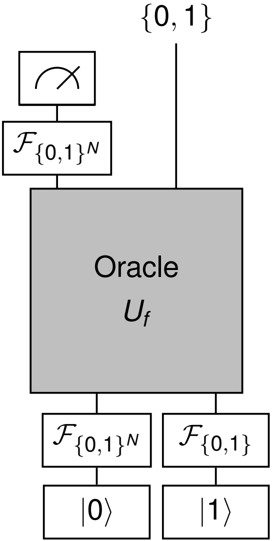
- Oracles are blackboxes with unknown internal structure.
- Most known quantum algorithms are constructed using quantum oracles, the Deutsch-Josza algorithm, Shor's algorithm, Grover's algorithm...
- Physical realizations of oracles place conditions on their "unknown" structure. (Unitarity in the quantum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

Main questions:

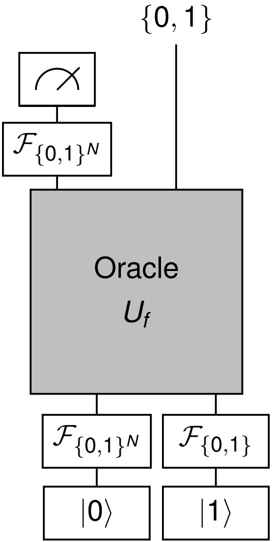
- What is the abstract structure of these oracles?
- Can we take advantage of this abstract setting to gain new insights?

Unitary Oracles

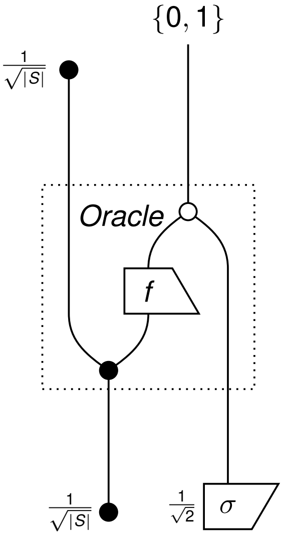
The traditional Deutsch-Joza circuit is:



Unitary Oracles

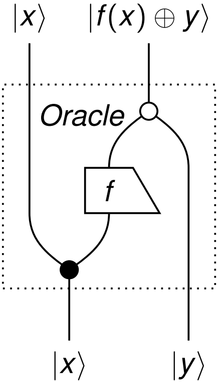


Here is its abstract structure:



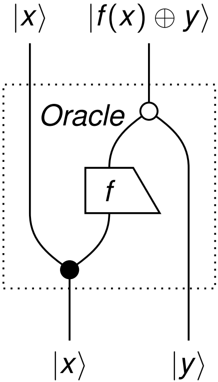
Unitary Oracles

This is the oracle's internal structure:



Unitary Oracles

This is the oracle's internal structure:

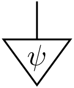


Theorem

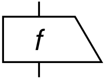
Oracles with this abstract structure are unitary in general.

Categorical Quantum Information

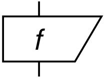
View quantum information in the context of the dagger-compact category **FHilb**



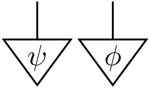
is a state $\psi : I \to \mathcal{H}$



is a linear map $f : A \to B$.



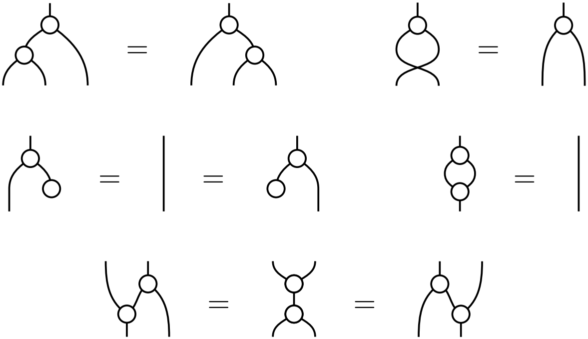
is the adjoint $f^\dagger : B \to A$.



is the composite state $I \to \psi \otimes \phi$

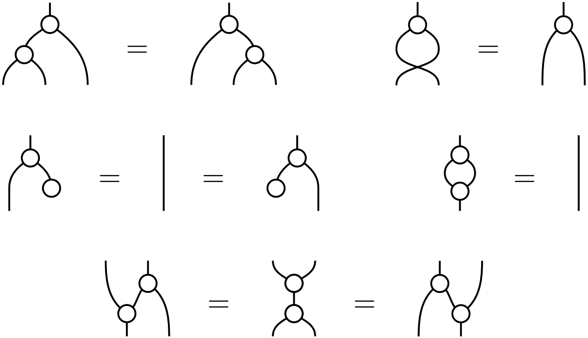
Categorical Quantum Information

Definition: A special †-Frobenius algebra (A, ,) obeys:



Categorical Quantum Information

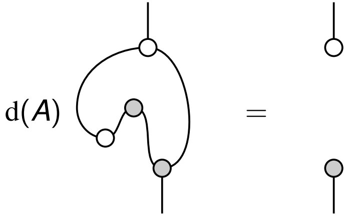
Definition: A special †-Frobenius algebra (A, , ) obeys:



This represents the abstract structure of an *observable* or generalized basis.

Complementary observables

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



Complementary observables

Finite abelian groups give complementary observables in **FHilb**

- Copying

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

 $:: |g\rangle \mapsto 1$

- Group multiplication

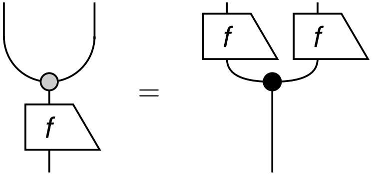
 $:: |g_1\rangle \otimes |g_2\rangle \mapsto \frac{1}{\sqrt{D}} |g_1 \oplus g_2\rangle$

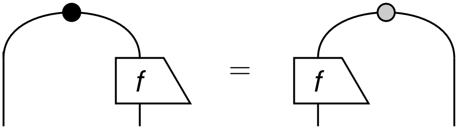
 $:: 1 \mapsto \sqrt{D}|0\rangle$

Classical Maps

Definition:

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

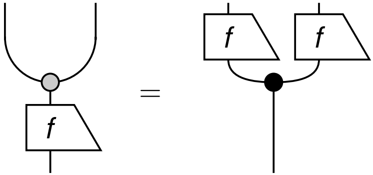


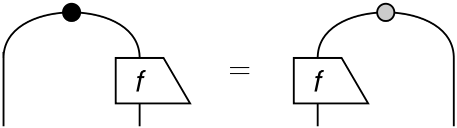


Classical Maps

Definition:

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





These are self-conjugate comonoid homomorphisms.

Unitarity Theorem

- Three †-Frobenius algebras, $(\bullet, \circ, \bullet)$

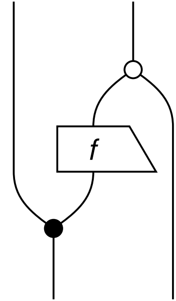
Unitarity Theorem

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

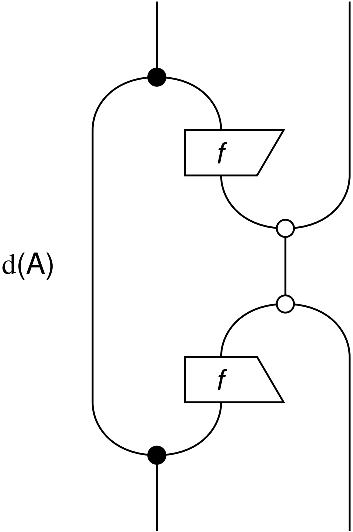
Unitarity Theorem

- Three †-Frobenius algebras, ($\bullet$, $\circ$, $\bullet$)
- A pair are complementary ($\bullet$ and $\circ$)
- A classical map $f : (A, \ , \ ) \to (B, \ , \ )$

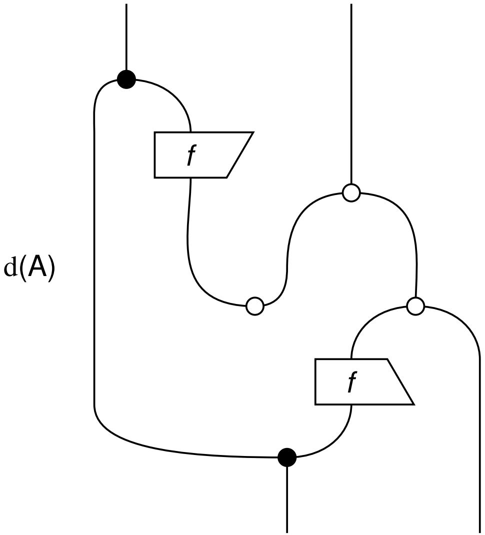
Produce the *unitary* morphism:

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

Abstract proof of unitarity

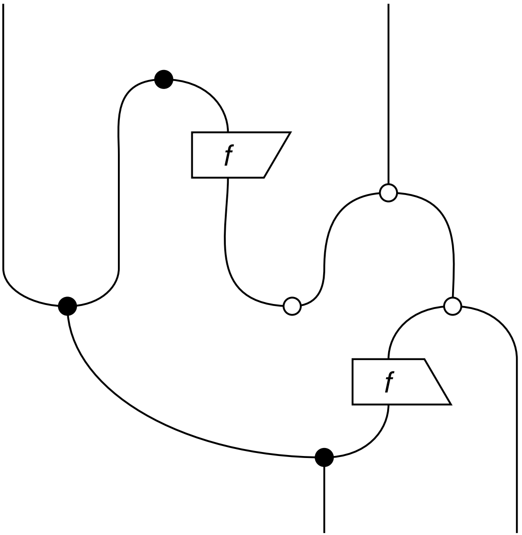


Abstract proof of unitarity

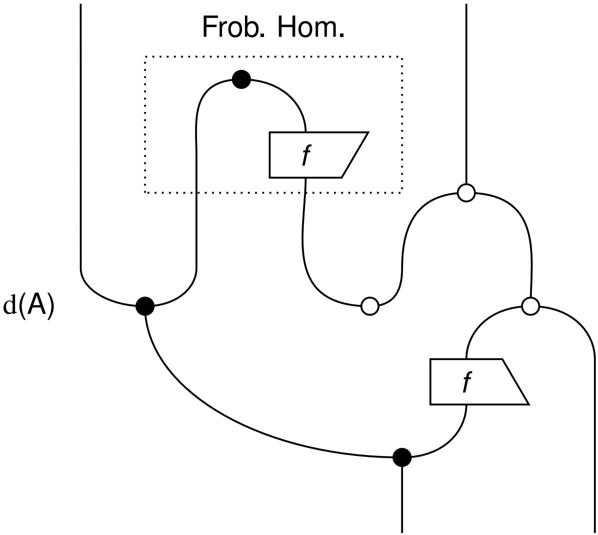


Abstract proof of unitarity

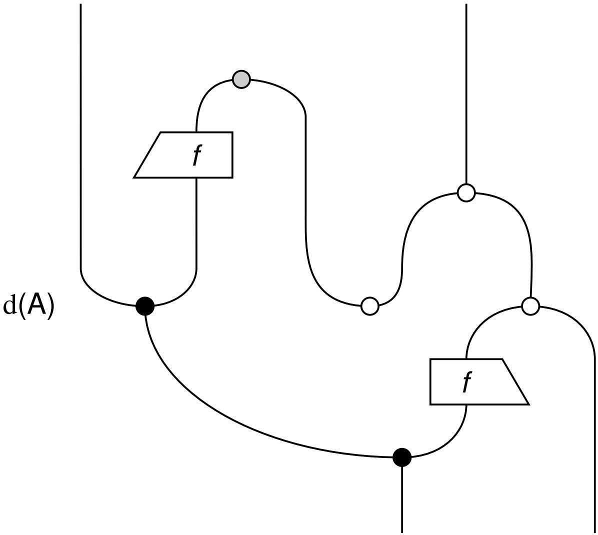
d(A)



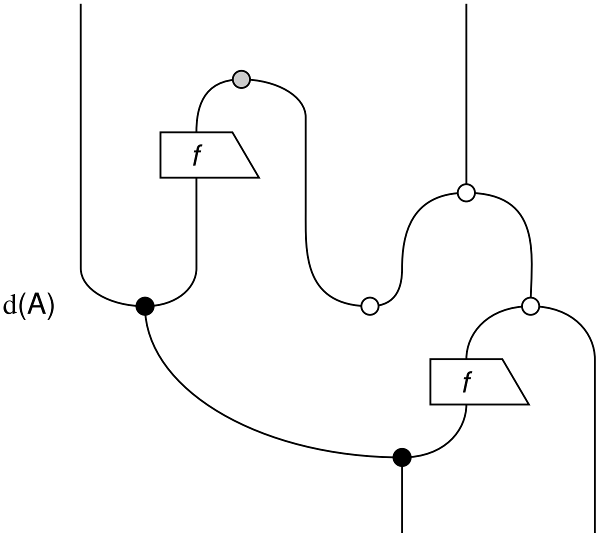
Abstract proof of unitarity



Abstract proof of unitarity

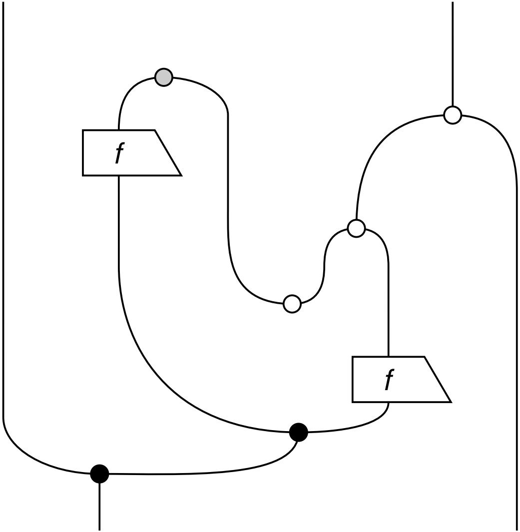


Abstract proof of unitarity

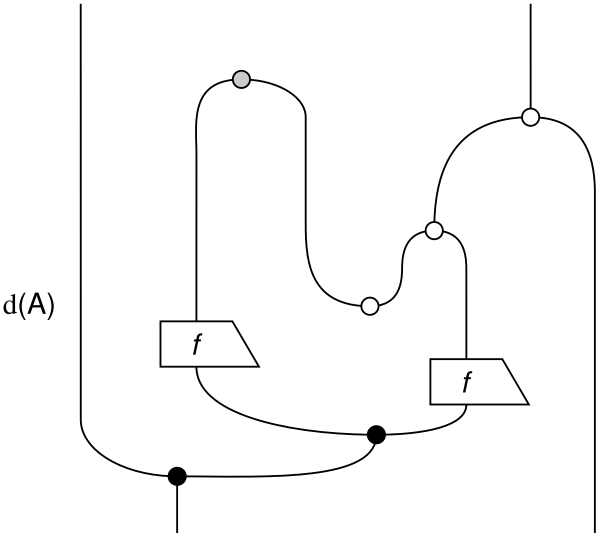


Abstract proof of unitarity

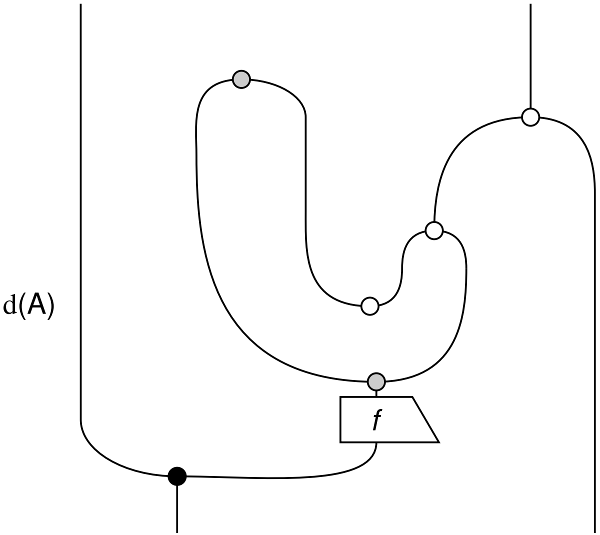
$\mathrm{d}(\mathsf{A})$



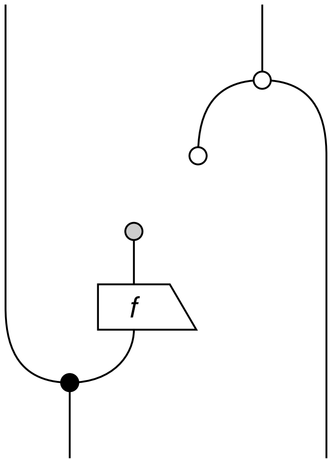
Abstract proof of unitarity



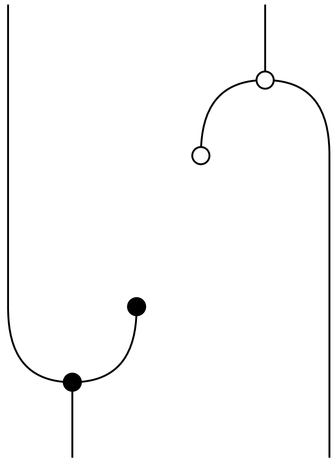
Abstract proof of unitarity



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?

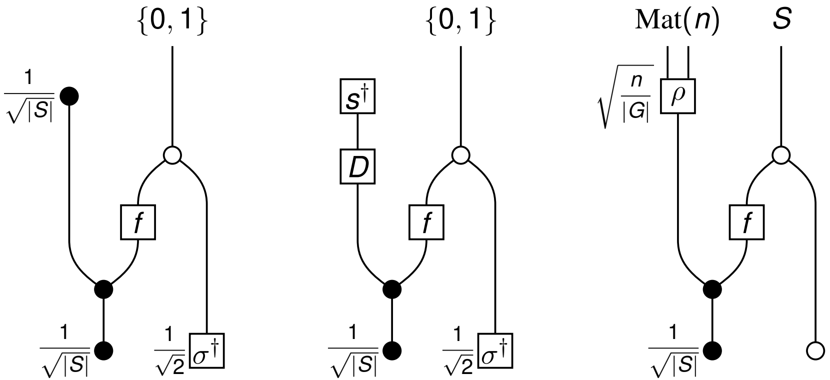
Unitary Oracles

- 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.

  Details in [Zeng & Vicary 2014]

  Up next
- Quantum algorithms: The old, the generalized and the new.

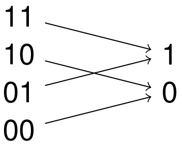
Quantum algorithms: old, generalized and new



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

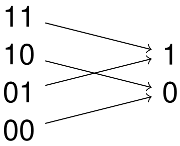
The Deutsch-Jozsa Algorithm

- Blackbox function $f : \{0, 1\}^N \rightarrow \{0, 1\}$ is *balanced* when it takes each possible value the same number of times



The Deutsch-Jozsa Algorithm

- Blackbox function $f : \{0,1\}^N \to \{0,1\}$ is *balanced* when it takes each possible value the same number of times

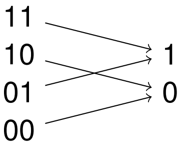


Definition (The Deutsch-Jozsa problem)

Given a blackbox function f promised to be either *constant* or *balanced*, identify which.

The Deutsch-Jozsa Algorithm

- Blackbox function $f : \{0,1\}^N \to \{0,1\}$ is *balanced* when it takes each possible value the same number of times



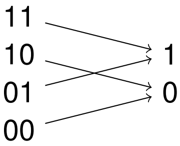
Definition (The Deutsch-Jozsa problem)

Given a blackbox function f promised to be either *constant* or *balanced*, identify which.

- Classically we require at most $2^{N-1} + 1$ queries of f

The Deutsch-Jozsa Algorithm

- Blackbox function $f : \{0,1\}^N \to \{0,1\}$ is *balanced* when it takes each possible value the same number of times



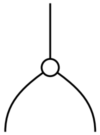
Definition (The Deutsch-Jozsa problem)

Given a blackbox function f promised to be either *constant* or *balanced*, identify which.

- Classically we require at most $2^{N-1}+1$ queries of f
- The quantum algorithm only requires a *single* query.

Group Algebras

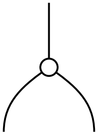
Recall the group multiplying observable:



$$G \times G \xrightarrow{m} G$$

Group Algebras

Recall the group multiplying observable:

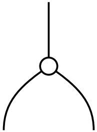


$$G \otimes G \xrightarrow{m} G$$

A *one-dimensional representation* $G \xrightarrow{\rho} \mathbb{C}$ is:

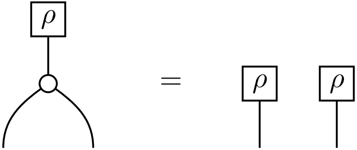
Group Algebras

Recall the group multiplying observable:



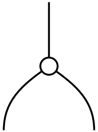
$$G \otimes G \xrightarrow{m} G$$

A *one-dimensional representation* $G \xrightarrow{\rho} \mathbb{C}$ is:



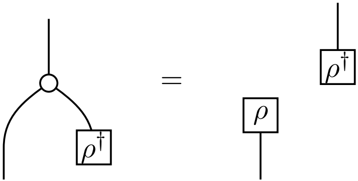
Group Algebras

Recall the group multiplying observable:



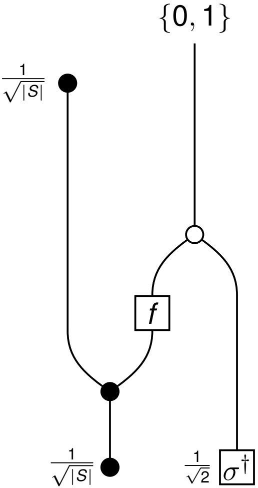
$$G \otimes G \xrightarrow{m} G$$

A *one-dimensional representation* $G \xrightarrow{\rho} \mathbb{C}$ is:



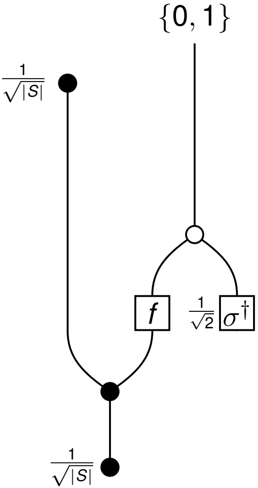
The adjoint $\mathbb{C} \xrightarrow{\rho} G$ is also copied on the lower legs.

CQM Deutsch-Jozsa



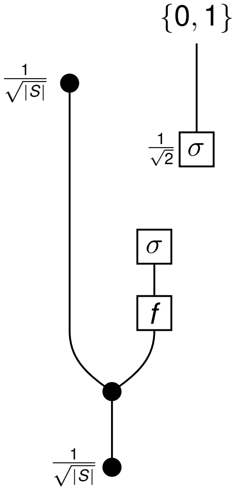
$\sigma(0) = 1$ and $\sigma(1) = -1$

CQM Deutsch-Jozsa



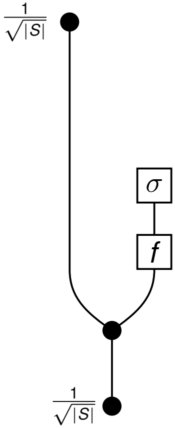
- Slide up $\sigma^\dagger$

CQM Deutsch-Jozsa



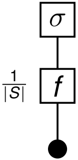
- Slide up $\sigma^\dagger$
- Pull $\sigma^\dagger$ through the whitedot

CQM Deutsch-Jozsa



- Slide up $\sigma^\dagger$
- Pull $\sigma^\dagger$ through the whitedot
- Neglect the right-side system

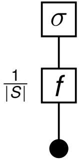
CQM Deutsch-Jozsa



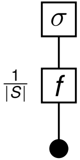
- Slide up $\sigma^\dagger$
- Pull $\sigma^\dagger$ through the whitedot
- Neglect the right-side system
- Spider law for the black dot

CQM Deutsch-Jozsa

Gives the amplitude for the input state $\frac{1}{\sqrt{|S|}} \sum_s |s\rangle$ to be in the σ state at measurement.

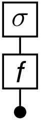


CQM Deutsch-Jozsa



Gives the amplitude for the input state $\frac{1}{\sqrt{|S|}} \sum_s |s\rangle$ to be in the σ state at measurement.

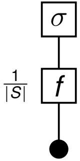
What if f is balanced?



$= \quad 0$

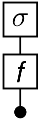
so the system is never measured in σ.

CQM Deutsch-Jozsa



Gives the amplitude for the input state $\frac{1}{\sqrt{|S|}}\sum_s |s\rangle$ to be in the σ state at measurement.

What if f is balanced?

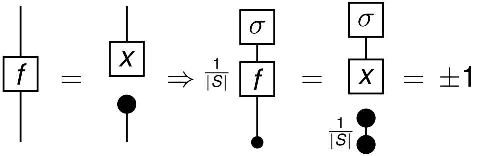


$= 0$

so the system is never measured in σ.

What if f is constant?

Then



So the system is always measured in σ.

Notes CQM Deutsch-Josza

- Verify: Abstractly verify the algorithm

Notes CQM Deutsch-Josza

- Verify: Abstractly verify the algorithm
- Generalize:
  - Abstract definition for balanced generalizes [Høyer 1999] and [Batty, Braunstein, Duncan 2006]. See [Vicary 2013]

Notes CQM Deutsch-Josza

- Verify: Abstractly verify the algorithm
- Generalize:
  - Abstract definition for balanced generalizes [Høyer 1999] and [Batty, Braunstein, Duncan 2006]. See [Vicary 2013]
  - The algorithm can be executed with complementary rather than strongly complementary observables

The Hidden Subgroup Problem

A *sneaky* function $G \xrightarrow{f} X$ is promised to be constant on the cosets of some normal subgroup $H \subseteq G$, and distinct otherwise. f factorizes as

$$\begin{tikzcd} G \arrow[r, two heads, "q"'] \arrow[rr, bend left, "f"] & G/H \arrow[r, tail, "s"'] & S \end{tikzcd},$$

Definition

Hidden subgroup problem Given a sneaky f, determine the subgroup H in $O(\log |G|)$ trials.

The Hidden Subgroup Problem

A *sneaky* function $G \xrightarrow{f} X$ is promised to be constant on the cosets of some normal subgroup $H \subseteq G$, and distinct otherwise. f factorizes as

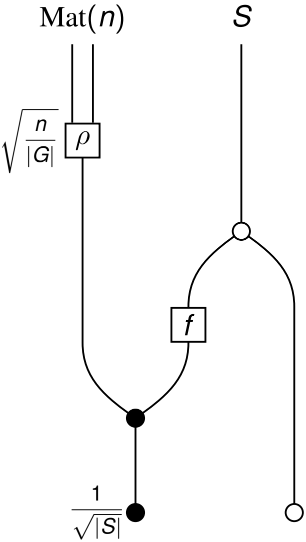
$$\begin{tikzcd} G \arrow[r, two heads, "q"'] \arrow[rr, bend left, "f"] & G/H \arrow[r, tail, "s"'] & S \end{tikzcd},$$

Definition

Hidden subgroup problem Given a sneaky f, determine the subgroup H in $O(\log |G|)$ trials.

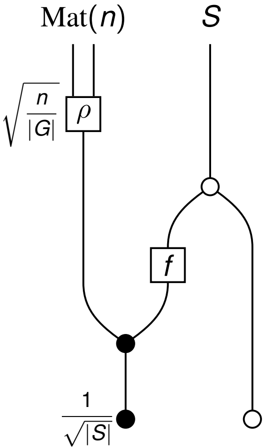
Shor's algorithm, discrete logarithms, graph isomorphism are cases

CQM Hidden Subgroup



Results:

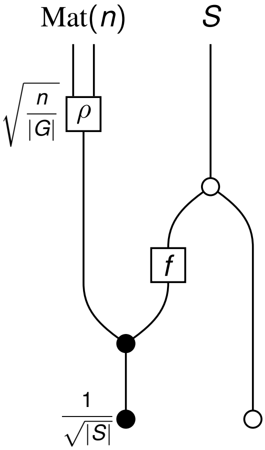
CQM Hidden Subgroup



Results:

- Verify that measurement returns irreps of G that factor G/H with probability proportional to the square of rep's dim. [Vicary 2013]

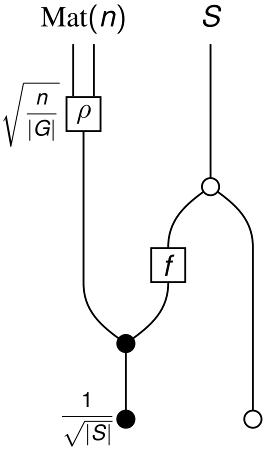
CQM Hidden Subgroup



Results:

- Verify that measurement returns irreps of G that factor G/H with probability proportional to the square of rep's dim. [Vicary 2013]
- No reliance on strong compl.

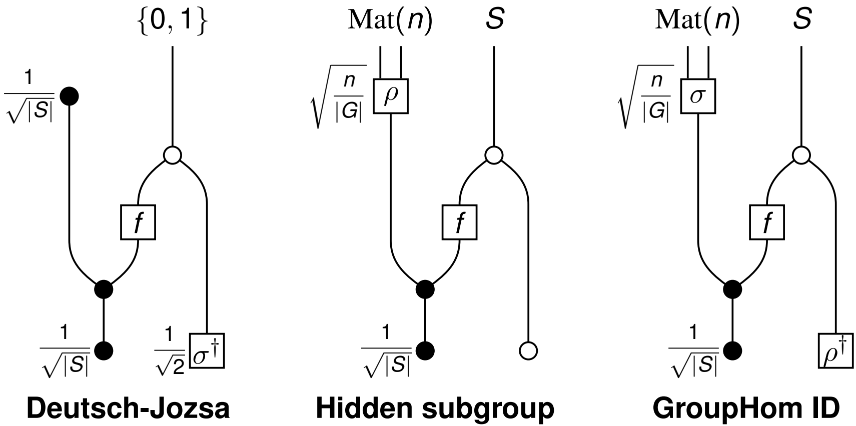
CQM Hidden Subgroup



Results:

- Verify that measurement returns irreps of G that factor G/H with probability proportional to the square of rep's dim. [Vicary 2013]
- No reliance on strong compl.
- Investigating improvements of input

Comparing Algorithms

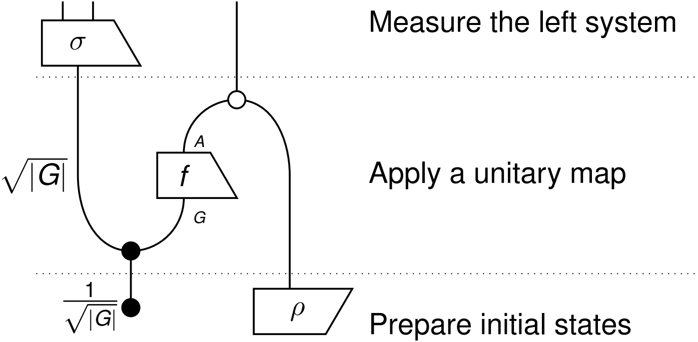


The group homomorphism identification problem

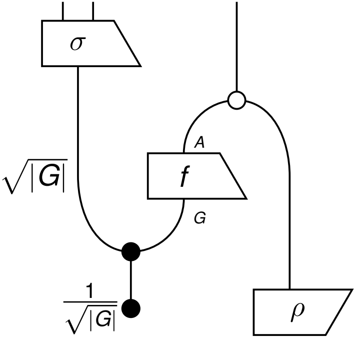
- Definition. (Group homomorphism identification problem) Given finite groups G and A where A is abelian, and a blackbox function $f : G \to A$ promised to be a group homomorphism, identify f.

The group homomorphism identification algorithm

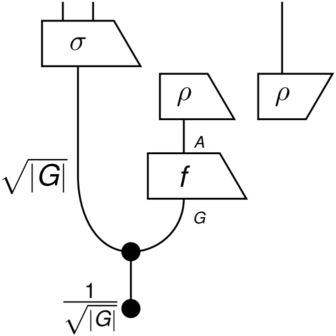
Case: Let A be a cyclic group $\mathbb{Z}_n$.



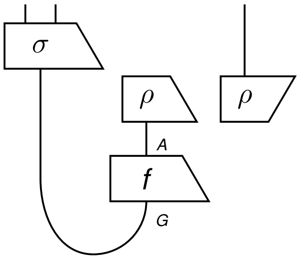
The group homomorphism identification algorithm



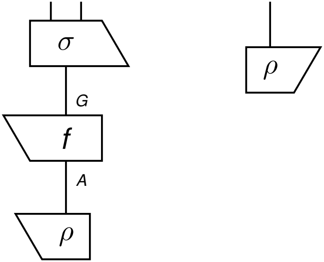
The group homomorphism identification algorithm



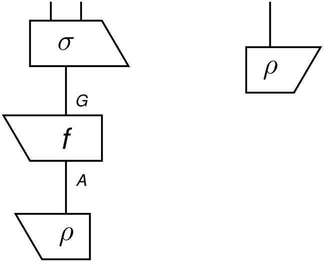
The group homomorphism identification algorithm



The group homomorphism identification algorithm

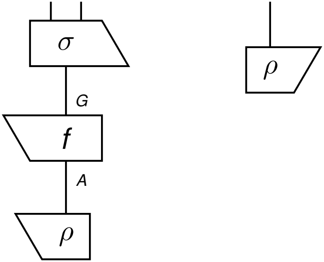


The group homomorphism identification algorithm



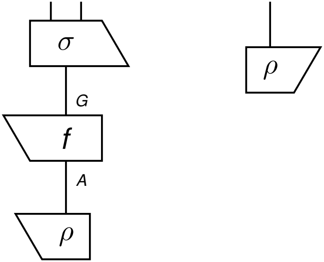
- $\rho \circ f$ is an irreducible representation of G.

The group homomorphism identification algorithm



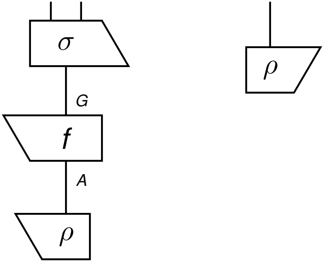
- $\rho \circ f$ is an irreducible representation of G.
- Choose ρ to be a faithful representation of A.

The group homomorphism identification algorithm



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

See [Zeng & Vicary 2014]

Grover's Algorithm

Background:

- Grover's quantum algorithm finds a single marked element of a finite set in $O(\sqrt{N})$ trials, vs classical $O(N)$.

Grover's Algorithm

Background:

- Grover's quantum algorithm finds a single marked element of a finite set in $O(\sqrt{N})$ trials, vs classical $O(N)$.
- If exactly $\frac{1}{4}$ of the elements are marked, it can find a marked element in a *single trial*.

Grover's Algorithm

Background:

- Grover's quantum algorithm finds a single marked element of a finite set in $O(\sqrt{N})$ trials, vs classical $O(N)$.
- If exactly $\frac{1}{4}$ of the elements are marked, it can find a marked element in a *single trial*.

In [Vicary 2013]:

- Verification of the single-shot Grover's algorithm.

Grover's Algorithm

Background:

- Grover's quantum algorithm finds a single marked element of a finite set in $O(\sqrt{N})$ trials, vs classical $O(N)$.
- If exactly $\frac{1}{4}$ of the elements are marked, it can find a marked element in a *single trial*.

In [Vicary 2013]:

- Verification of the single-shot Grover's algorithm.
- The CQM perspective highlights the structural role of the group $\mathbb{Z}_2$.

Grover's Algorithm

Background:

- Grover's quantum algorithm finds a single marked element of a finite set in $O(\sqrt{N})$ trials, vs classical $O(N)$.
- If exactly $\frac{1}{4}$ of the elements are marked, it can find a marked element in a *single trial*.

In [Vicary 2013]:

- Verification of the single-shot Grover's algorithm.
- The CQM perspective highlights the structural role of the group $\mathbb{Z}_2$.
- Changing the finite group gives 'multicoloured' quantum search algorithms which achieve tasks that ordinary Grover search cannot.

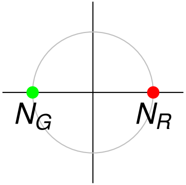
Examples

The generalized single-shot Grover algorithm finds colours whose ‘weighted phase’ *doesn’t* take twice the average value.

Examples

The generalized single-shot Grover algorithm finds colours whose 'weighted phase' *doesn't* take twice the average value.

Suppose $f : S \to \mathbb{Z}_2 \simeq \{R, G\}$, $\sigma = (1, -1)$. Essentially, red and green balls at ± 1.



For one colour to take twice the average value we require a 3:1 ratio.

Rarer colour returned in a single query. Standard result from Grover theory.

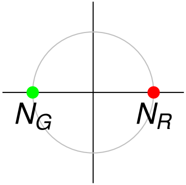
Examples

The generalized single-shot Grover algorithm finds colours whose 'weighted phase' *doesn't* take twice the average value.

Suppose $f : S \to \mathbb{Z}_2 \simeq \{R, G\}$, $\sigma = (1, -1)$.
Essentially, red and green balls at ± 1.

For one colour to take twice the average value we require a 3:1 ratio.

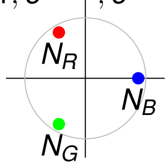
Rarer colour returned in a single query.
Standard result from Grover theory.



Now suppose $f : S \to \mathbb{Z}_3 \simeq \{R, G, B\}$, $\sigma = (1, e^{2\pi i/3}, e^{4\pi i/3})$.
Red, green, blue balls at $e^{2n\pi i/3}$.

For one colour to take twice the average value we require a 4:1:1 ratio.

A rarer colour returned in a single query.
Cannot be done with ordinary Grover algorithm.



Concluding Grover's

- We can verify and generalize Grover's algorithm with the CQM framework.
  [Vicary 2013]

Concluding Grover's

- We can verify and generalize Grover's algorithm with the CQM framework.
  [Vicary 2013]

- Since Grover's forms the basis for other quantum subroutines, e.g. amplitude amplification, amplitude estimation, and quantum minimization algorithms, etc. This is an important building block.

Leveraging generality: other categories

- Relate Unitary Oracles to the resistor structure in signal-flow calculus [Zeng & Vicary 2014]
- Define these algorithms in Rel

- We should think about computational speedup as a property of a physical theory in much the same way that we think about contextuality and non-locality.

Conclusions and Frontiers

Successes

- Categorical quantum mechanics give a handle on the abstract structure of quantum algorithms:

Conclusions and Frontiers

Successes

- Categorical quantum mechanics give a handle on the abstract structure of quantum algorithms:
- To develop new quantum algorithms

Conclusions and Frontiers

Successes

- Categorical quantum mechanics give a handle on the abstract structure of quantum algorithms:
- To develop new quantum algorithms
- To investigate what structures in QM lead to speedups

Conclusions and Frontiers

Successes

- Categorical quantum mechanics give a handle on the abstract structure of quantum algorithms:
- To develop new quantum algorithms
- To investigate what structures in QM lead to speedups

Challenges

- Capture non-oracle algorithms within the framework
- Capture non-single-shot algorithms

Conclusions and Frontiers

Successes

- Categorical quantum mechanics give a handle on the abstract structure of quantum algorithms:
- To develop new quantum algorithms
- To investigate what structures in QM lead to speedups

Challenges

- Capture non-oracle algorithms within the framework
- Capture non-single-shot algorithms

Particular current work

- Capture new quantum machine learning algorithms

Conclusions and Frontiers

Successes

- Categorical quantum mechanics give a handle on the abstract structure of quantum algorithms:
- To develop new quantum algorithms
- To investigate what structures in QM lead to speedups

Challenges

- Capture non-oracle algorithms within the framework
- Capture non-single-shot algorithms

Particular current work

- Capture new quantum machine learning algorithms
- Connect quantum algorithms to NLP through compact categories

The closest vector problem

The closest vector problem

Definition

Given vector s and a set of M vectors $U = \{\vec{v}_0, \vec{v}_1, ...\vec{v}_{M-1}\}$ the *closest vector problem* asks one to determine which v_i has the smallest inner product distance with s. We will assume that all vectors are N-dimensional.

The closest vector problem

Definition

Given vector s and a set of M vectors $U = \{\vec{v}_0, \vec{v}_1, \ldots \vec{v}_{M-1}\}$ the *closest vector problem* asks one to determine which v_i has the smallest inner product distance with s. We will assume that all vectors are N-dimensional.

- Appears in clustering, text classification, phrase/word similarity, sentiment analysis, etc.

The closest vector problem

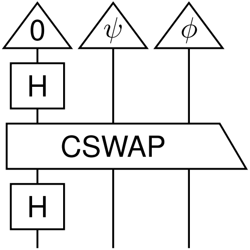
Definition

Given vector s and a set of M vectors $U = \{\vec{v}_0, \vec{v}_1, ...\vec{v}_{M-1}\}$ the *closest vector problem* asks one to determine which v_i has the smallest inner product distance with s. We will assume that all vectors are N-dimensional.

- Appears in clustering, text classification, phrase/word similarity, sentiment analysis, etc.
- Classical algorithms for this problem have complexity $\mathcal{O}(MN)$.

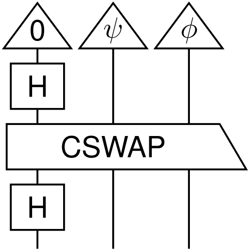
A quantum algorithm for the closest vector problem

Definition (SWAP Test)



A quantum algorithm for the closest vector problem

Definition (SWAP Test)

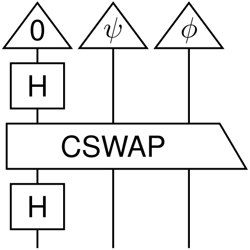


Hadamard Transform:

$$H :: |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

A quantum algorithm for the closest vector problem

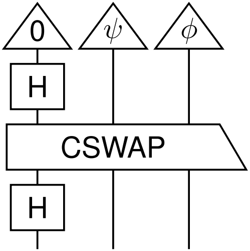
Definition (SWAP Test)



Resulting state: $\frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle)$,

A quantum algorithm for the closest vector problem

Definition (SWAP Test)

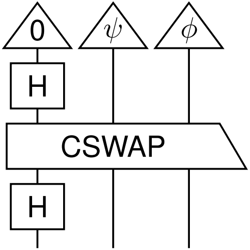


Resulting state: $\frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle)$,
Probability of measuring the left system to be zero is

$$1/2 - |\langle\phi|\psi\rangle|^2/2.$$

A quantum algorithm for the closest vector problem

Definition (SWAP Test)



Resulting state: $\frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle)$,
Probability of measuring the left system to be zero is

$$1/2 - |\langle\phi|\psi\rangle|^2/2.$$

Takeaway: In a single step we can encode the inner product of two vectors.

A quantum algorithm for the closest vector problem

qCVECT has the following steps:

1. Add ancillary qubits $|i\rangle$ (for indexing) and $|\psi_i\rangle$ (for the SWAP test) and apply the **SWAP test** (without measurement) for each pair (s, v_i).

A quantum algorithm for the closest vector problem

qCVECT has the following steps:

1. Add ancillary qubits $|i\rangle$ (for indexing) and $|\psi_i\rangle$ (for the SWAP test) and apply the **SWAP test** (without measurement) for each pair (s, v_i).
2. Perform coherent **amplitude estimation** to determine the amplitude of the zero state for the ancillary qubits $|\psi_0\rangle, |\psi_1\rangle, \ldots$. This stores the distances estimates in a qubit string without measurement. [Wiebe et. al. 2014]

A quantum algorithm for the closest vector problem

qCVECT has the following steps:

1. Add ancillary qubits $|i\rangle$ (for indexing) and $|\psi_i\rangle$ (for the SWAP test) and apply the **SWAP test** (without measurement) for each pair (s, v_i).
2. Perform coherent **amplitude estimation** to determine the amplitude of the zero state for the ancillary qubits $|\psi_0\rangle, |\psi_1\rangle, \ldots$. This stores the distances estimates in a qubit string without measurement. [Wiebe et. al. 2014]
3. Use the Dürr-Hoyer **minimization** algorithm to return the i which minimizes $\left(1 - |\langle v_i|s\rangle|^2\right)$.

A quantum algorithm for the closest vector problem

qCVECT has the following steps:

1. Add ancillary qubits $|i\rangle$ (for indexing) and $|\psi_i\rangle$ (for the SWAP test) and apply the **SWAP test** (without measurement) for each pair (s, v_i).
2. Perform coherent **amplitude estimation** to determine the amplitude of the zero state for the ancillary qubits $|\psi_0\rangle, |\psi_1\rangle, \ldots$. This stores the distances estimates in a qubit string without measurement. [Wiebe et. al. 2014]
3. Use the Dürr-Hoyer **minimization** algorithm to return the i which minimizes $\left(1 - |\langle v_i|s\rangle|^2\right)$.

The runtime is $\mathcal{O}(Me^{-1/2})$ and a slightly more complicated version runs in almost $\mathcal{O}(\sqrt{M}e^{-1/2})$

Complexity Comparisons

- TIME: Classification tasks can be performed in runtimes that are independent of the dimension of the meaning space.

Complexity Comparisons

- TIME: Classification tasks can be performed in runtimes that are independent of the dimension of the meaning space.
- SPACE: Exponential reduction in required space. An N-dimensional classical vector requires $\log_2 N$ qubits.

Complexity Comparisons

- TIME: Classification tasks can be performed in runtimes that are independent of the dimension of the meaning space.
- SPACE: Exponential reduction in required space. An N-dimensional classical vector requires $\log_2 N$ qubits.
  - DisCo becomes more attractive as large order tensors are feasibly implemented

Complexity Comparisons

- TIME: Classification tasks can be performed in runtimes that are independent of the dimension of the meaning space.
- SPACE: Exponential reduction in required space. An N-dimensional classical vector requires $\log_2 N$ qubits.
  - DisCo becomes more attractive as large order tensors are feasibly implemented
  - Secrecy advantages. Classification task requires less queries than are necessary to reconstruct the classifying clusters.

Thanks!

CQM Algorithms References:

Vicary, *The Topology of Quantum Algorithms* arXiv:1209.3917

Zeng & Vicary *Abstract structure of unitary oracles for quantum algorithms* arXiv:1406.1278