Title: Higher-order interference doesn't help in searching for a needle in a haystack

Date: Aug 05, 2016 02:00 PM

URL: http://pirsa.org/16080030

Abstract:

Higher-order interference doesn't help in finding a needle in a haystack

Ciarán Lee

Joint work with John Selby

arXiv:1604.03118 & arXiv:1510.04699

Consequences of higher-order interference?

- Absence of third-order interference, in conjunction with other physical principles, uniquely specifies quantum theory.
- Does post-quantum interference imply post-quantum features? Information-theoretic advantages?

The search problem

- Items indexed $1, .., x, .., N$, with x the 'marked' item.
- One has access to an **oracle**, which when asked if item $i = x$ returns 'yes' or 'no'.
- $f : \{1, \ldots, N\} \to \{0, 1\}$ satisfies $f(i) = 1$ if and only if $i = x$.
- What is minimal number of queries to this oracle to find x in the worst case?

The search problem

- Classical algorithms require $O(N)$ queries to find marked item in worst case.
- There exists a quantum algorithm which finds item in $O(\sqrt{N})$ queries.
- $O(\sqrt{N})$ queries is **optimal** for quantum theory.

Quantum oracles

In quantum theory, an oracle corresponds to a controlled unitary transformation

$$U|i\rangle|q\rangle = |i\rangle|q \oplus f(i)\rangle$$

where $f : \{1, \ldots, N\} \to \{0, 1\}$ satisfies $f(i) = 1$ if and only if $i = x$.

Quantum oracles

In quantum theory, an oracle corresponds to a controlled unitary transformation

$$U|i\rangle|q\rangle = |i\rangle|q \oplus f(i)\rangle$$

where $f : \{1, \ldots, N\} \to \{0, 1\}$ satisfies $f(i) = 1$ if and only if $i = x$.

Quantum oracles

- Inputting $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ results in a "kicked-back" phase:

$$U|i\rangle|-\rangle = (-1)^{f(i)}|i\rangle|-\rangle$$

- Discarding $|-\rangle$ reduces the action of the oracle to

$$O_x|i\rangle = (-1)^{f(i)}|i\rangle.$$

Operational theories and Physical principles

- We study the connection between higher-order interference and the search problem in the setting of operational theories.

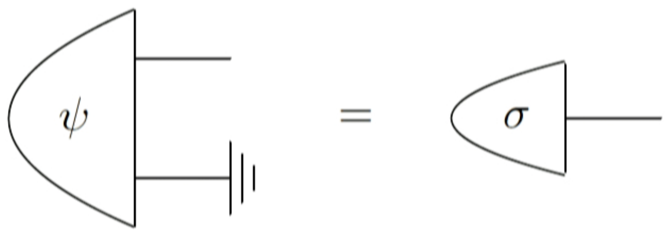
- An operational theory specifies a set of laboratory devices which can be connected together to form experiments and assigns probabilities to experimental outcomes.

Principle 1: Purification

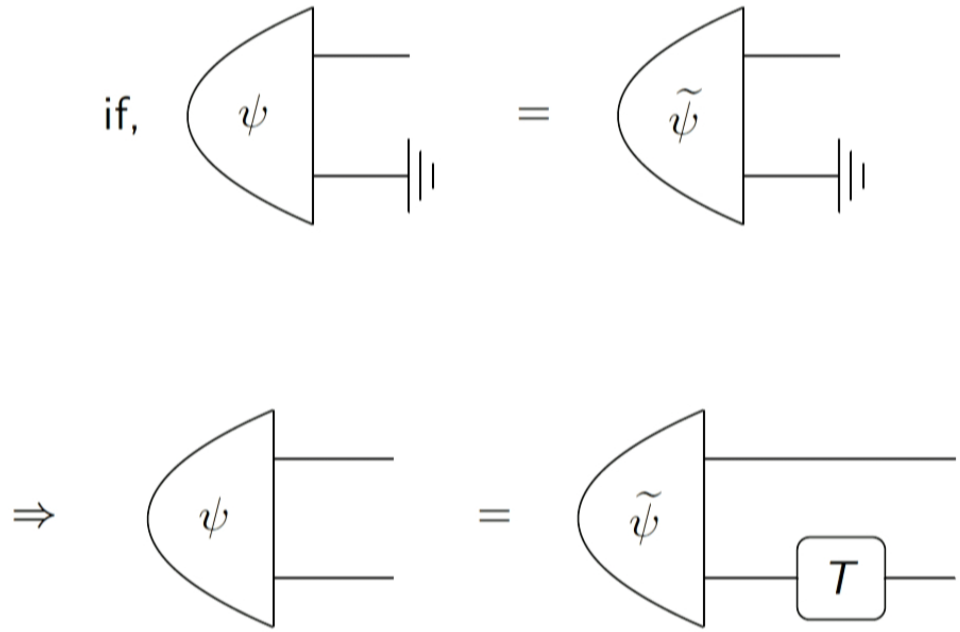
- Process $\{E_j\}_{j \in Y}$ refines process $\{F_k\}_{k \in X}$ if $F_k = \sum_{j \in X_k} E_j$.
- A process is pure if it has trivial refinements.
- A pure process is one about which we have "maximal information".

Principle 1: Purification

All states can be ‘purified’ by including an appropriate environment:

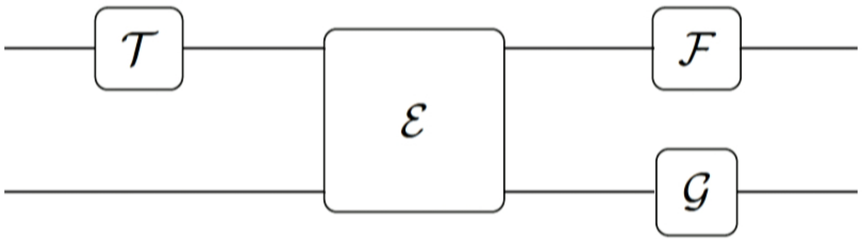


Principle 1: Purification

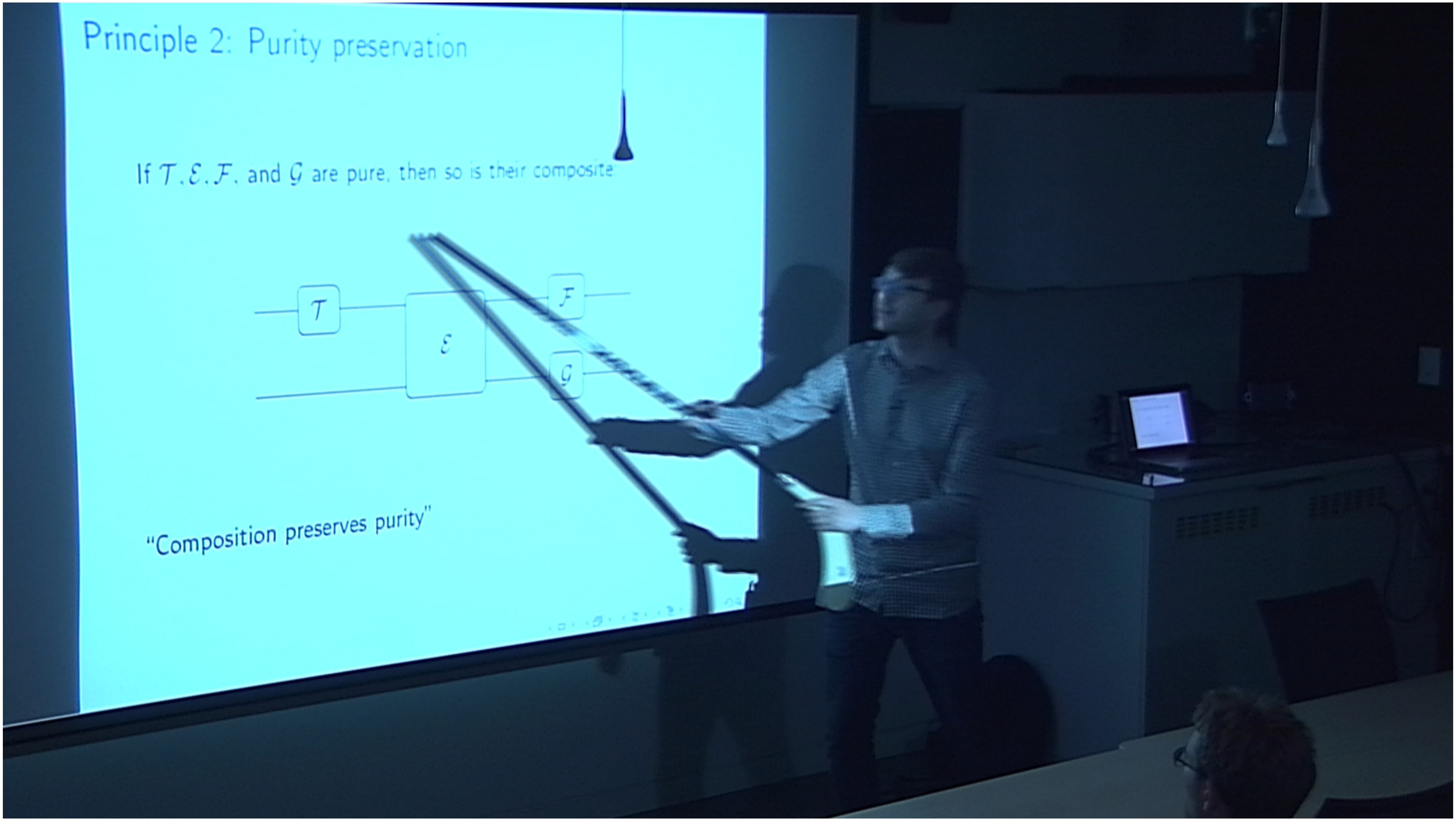


Principle 2: Purity preservation

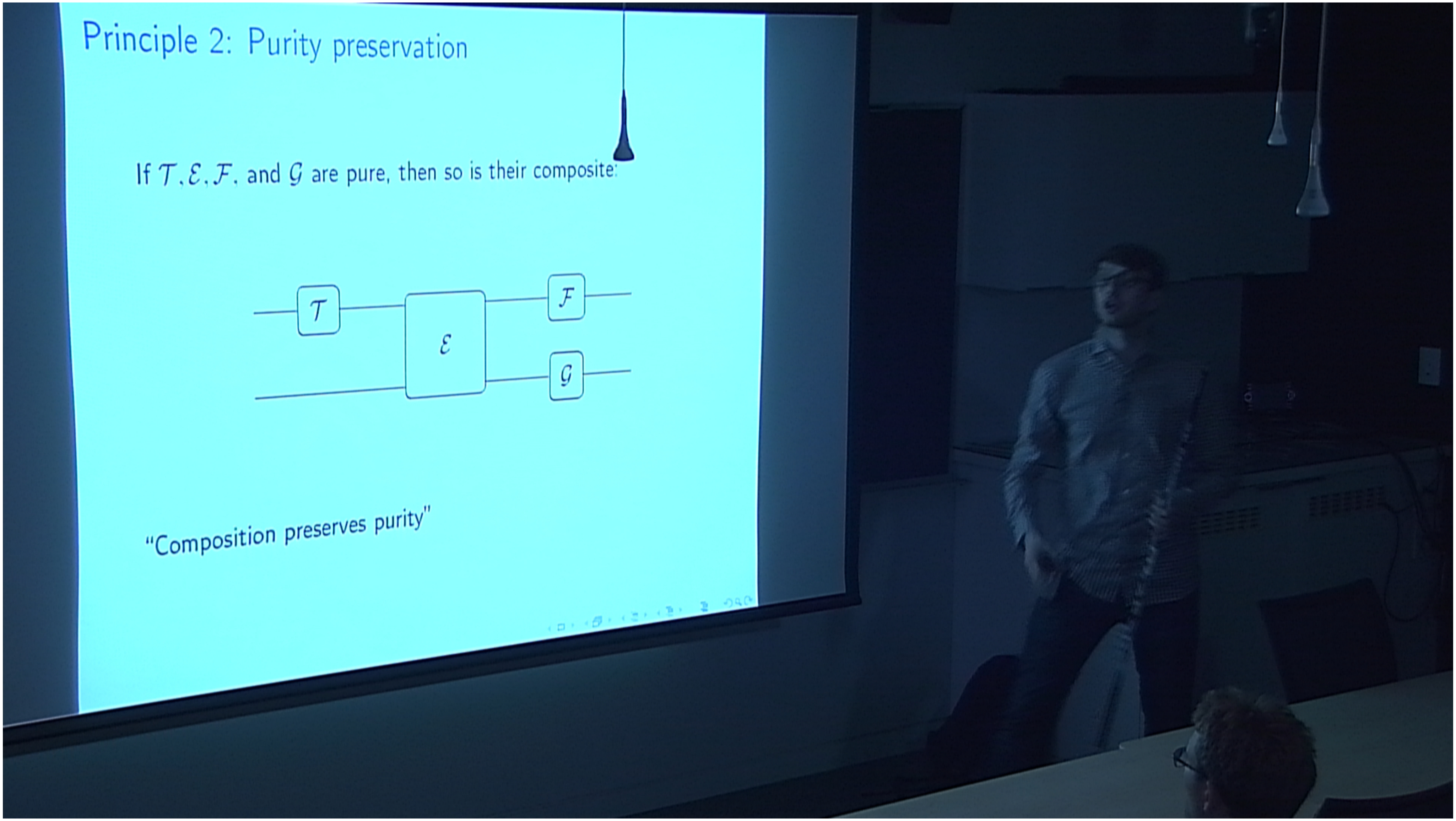
If $\mathcal{T}, \mathcal{E}, \mathcal{F}$, and $\mathcal{G}$ are pure, then so is their composite:



"Composition preserves purity"



Principle 2: Purity preservation
If $\mathcal{T}$, $\mathcal{E}$, $\mathcal{F}$, and $\mathcal{G}$ are pure, then so is their composite:
$\mathcal{T}$
$\mathcal{E}$
$\mathcal{F}$
$\mathcal{G}$
"Composition preserves purity"



Principle 2: Purity preservation
If $\mathcal{T}, \mathcal{E}, \mathcal{F}$, and $\mathcal{G}$ are pure, then so is their composite:
$\mathcal{T}$
$\mathcal{E}$
$\mathcal{F}$
$\mathcal{G}$
"Composition preserves purity"

Principle 3: Strong symmetry

Given two sets of perfectly distinguishable pure states

$$\{\sigma_i\} \text{ and } \{\rho_i\}$$

there exists reversible $\mathcal{T}$ such that:

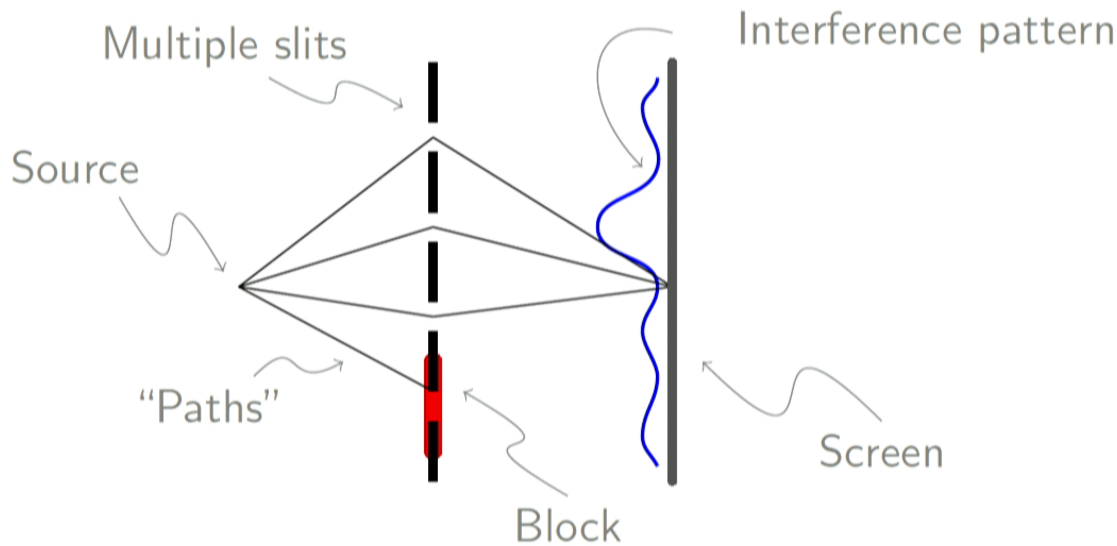
Principle 3: Strong symmetry

Given two sets of perfectly distinguishable pure states

$$\{\sigma_i\} \text{ and } \{\rho_i\}$$

there exists reversible $\mathcal{T}$ such that:

Higher-order interference in the presence of these principles



Blocking some slits, but leaving subset $I \subseteq \{1, \ldots, N\}$ open, corresponds to applying the projector P_I, satisfying $P_I P_J = P_{I \cap J}$.

Higher-order interference in the presence of these principles

Maximal order of interference h corresponds to:

$$\mathbb{1}_N = \sum_{\substack{I \subseteq \mathbf{N} \\ |I| \leq h}} (-1)^{h-|I|} \binom{N-|I|-1}{h-|I|} P_I$$

The case of $N = h+1$ corresponds to $(-1)^{h-|I|}$. In quantum theory, this is:

$$\mathbb{1}_N = \sum_{i<j} P_{\{ij\}} - (N-2) \sum_i P_{\{i\}},$$

Higher-order interference in the presence of these principles

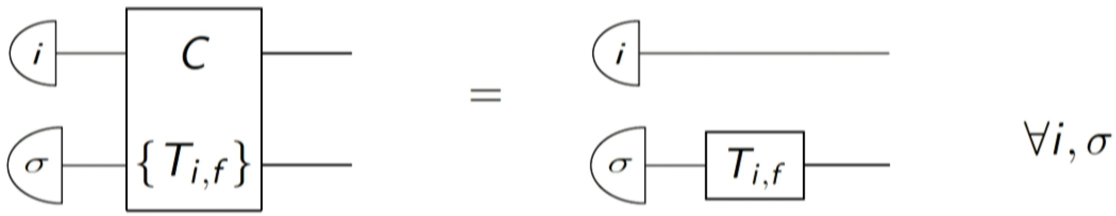
Maximal order of interference h corresponds to:

$$\mathbb{1}_N = \sum_{\substack{I \subseteq \mathbf{N} \\ |I| \leq h}} (-1)^{h-|I|} \binom{N-|I|-1}{h-|I|} P_I$$

The case of $N = h + 1$ corresponds to $(-1)^{h-|I|}$. In quantum theory, this is:

$$\mathbb{1}_N = \sum_{i<j} P_{\{ij\}} - (N-2) \sum_i P_{\{i\}},$$

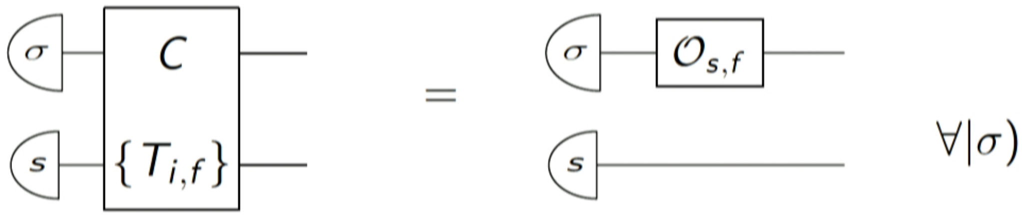
Oracles in operational theories



Making the set of transformations $\{T_{i,f(i)}\}$ depend on the function $f : \{i\} \to \{0,1\}$ encoding the search problem allows us to define a computational oracle.

Oracles in operational theories

There exists a state s such that:

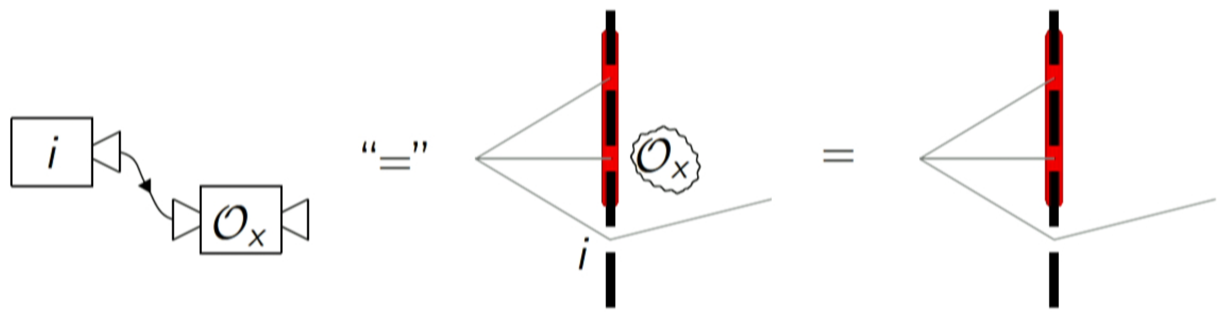


Moreover, $\mathcal{O}_{s,f}$ is phase transformation:

Setting up the search problem in operational theories

- In quantum theory, to query the oracle about i one applies the oracle to state $|i\rangle\langle i|$.
- $|i\rangle\langle i|$ can be prepared by passing a uniform superposition through an N-slit experiment with all but the ith slit blocked.
- The oracle can be implemented by placing a phase shifter behind slit x.

Setting up the search problem in operational theories



1. $\mathcal{O}_x P_I = P_I$, if $x \notin I$ or $|I| = 1$

2. $\mathcal{O}_x$ can act non-trivially on P_I with $x \in I$ and $|I| > 1$, but must satisfy $\mathcal{O}_x P_I = P_I \mathcal{O}_x$, for all P_I

Setting up the search problem in operational theories

The requirement $\mathcal{O}_x P_I = P_I \mathcal{O}_x$ ensures one cannot gain any information about item i when querying with a state that doesn't pass through slit i, i.e. a state s such that $P_I s = s$ where $i \notin I$.

Setting up the search problem in operational theories

A reversible transformation is a *search oracle*, denoted $\mathcal{O}_x$, if and only if:

i) $\mathcal{O}_x P_I = P_I$ for all $x \notin I$ or $|I| = 1$ and,

ii) $\mathcal{O}_x P_I = P_I \mathcal{O}_x$, for all P_I.

Setting up the search problem in operational theories

Given a search oracle $\mathcal{O}_x$ and an arbitrary collection of reversible transformations $\{G_i\}$, what is the minimal $k \in \mathbb{N}$ such that

$$G_k \mathcal{O}_x G_{k-1} \dots G_1 \mathcal{O}_x s$$

can be found, with high probability, to be in the state x, for arbitrary input state s, averaged over all possible marked items?

Main result

In theories satisfying our principles, with (finite) maximal order of interference h, the number of queries needed to solve the search problem is

$$\Omega\left(\sqrt{\frac{N}{h}}\right).$$

Main result

In theories satisfying our principles, with (finite) maximal order of interference h, the number of queries needed to solve the search problem is

$$\Omega\left(\sqrt{\frac{N}{h}}\right).$$

Intuition for proof

The projector $P_{\{0,1\}}$ acts as:

$$P_{\{0,1\}} :: \begin{pmatrix} \rho_{00} & \rho_{01} & \rho_{02} \\ \rho_{10} & \rho_{11} & \rho_{12} \\ \rho_{20} & \rho_{21} & \rho_{22} \end{pmatrix} \mapsto \begin{pmatrix} \rho_{00} & \rho_{01} & 0 \\ \rho_{10} & \rho_{11} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

whilst the 'coherence-projector' $\omega_{\{0,1\}}$ acts as:

$$\omega_{\{0,1\}} :: \begin{pmatrix} \rho_{00} & \rho_{01} & \rho_{02} \\ \rho_{10} & \rho_{11} & \rho_{12} \\ \rho_{20} & \rho_{21} & \rho_{22} \end{pmatrix} \mapsto \begin{pmatrix} 0 & \rho_{01} & 0 \\ \rho_{10} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

That is, $\omega_{\{0,1\}}$ corresponds to the linear combination of projectors:

$$P_{\{0,1\}} - P_{\{0\}} - P_{\{1\}}.$$

Intuition for proof

- Can define coherence projectors for any I:

$$\omega_I := \sum_{\widetilde{I} \subseteq I} (-1)^{|I| + |\widetilde{I}|} P_{\widetilde{I}}.$$

- Alternate definition of maximal order h:

$$\mathbb{1}_N = \sum_{I, |I|=1}^{h} \omega_I, \text{ for all } N \geq h$$

Intuition for proof

Apply $\mathbb{1}_N$ to a state s

$$\Rightarrow s = \sum_{I,|I|=1}^{h} s_I, \text{ with } s_I := \omega_I s.$$

Think of s_I as the “coherences” between the slits in I.

Intuition for proof

- Oracle defined to act on projectors P_I, hence acts on ω_I.
- Oracle only acts non-trivially on parts of the decomposition "coherently linked" to x, i.e. those s_I with $x \in I$.

Intuition for proof

In quantum theory

$$\frac{\#\text{ terms coherently linked to x}}{\#\text{ total terms}} = \frac{N-1}{N^2} \sim \frac{1}{N}$$

Intuitively speaking, a quantum oracle can only "move" a given state a small amount in a single query.

Conclusion and further work

- As far as the search problem goes, all non-trivial (finite) orders of interference are asymptotically equivalent.
- Derivation of quadratic lower bound to search from simple physical principles similar to derivations of Tsirelson's bound from information causality, local orthogonality, etc.

Conclusion and further work

- Would existence of post-quantum interference compromise security of quantum protocols?

- Verification of delegated quantum computation needs to be proven secure against adversaries with post-quantum quantum dynamics, for example higher-order phase transformations.