



# *The Structure of Quantum Computation from Physical Principles*

John H. Selby & Ciarán M. Lee  
arXiv: 1510.04699, 1604.03118



“The structure of quantum computation...”



# “The structure of quantum computation...”

- ▶ Quantum departures from classicality
  - ▶ Non-locality
  - ▶ Contextuality
  - ▶ Computational speed-up



# “The structure of quantum computation...”

- ▶ Quantum departures from classicality
  - ▶ Non-locality
  - ▶ Contextuality
  - ▶ Computational speed-up



## “The structure of quantum computation...”

- ▶ Quantum departures from classicality
  - ▶ Non-locality
  - ▶ Contextuality
  - ▶ Computational speed-up
- ▶ What provides the quantum speed-up?



## “The structure of quantum computation...”

- ▶ Quantum departures from classicality
  - ▶ Non-locality
  - ▶ Contextuality
  - ▶ Computational speed-up
- ▶ What provides the quantum speed-up?
- ▶ Why is there not more of a speed-up?



## “The structure of quantum computation...”

- ▶ Quantum departures from classicality
  - ▶ Non-locality
  - ▶ Contextuality
  - ▶ Computational speed-up
- ▶ What provides the quantum speed-up?
- ▶ Why is there not more of a speed-up?
- ▶ How can we design optimal algorithms?



“...from physical principles.”





“...from physical principles.”

Internal perspective:

Standard quantum formalism

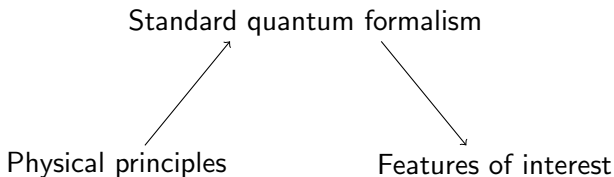


Features of interest



“...from physical principles.”

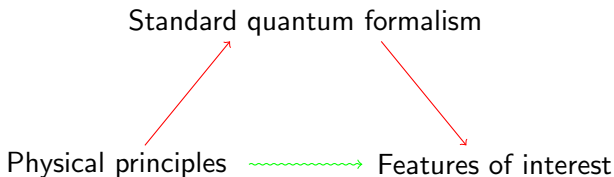
Reconstruction perspective:





“...from physical principles.”

External perspective:





## Analogy: Study of non-local correlations

- ▶ Why are quantum correlations non-local?



## Analogy: Study of non-local correlations

- ▶ Why are quantum correlations non-local?
- ▶ Why are quantum correlations not more non-local?



## Analogy: Study of non-local correlations

- ▶ Why are quantum correlations non-local?
- ▶ Why are quantum correlations not more non-local?
- ▶ Information causality and Tsirelson's bound



## Analogy: Study of non-local correlations

- ▶ Why are quantum correlations non-local?
- ▶ Why are quantum correlations not more non-local?
- ▶ Information causality and Tsirelson's bound
- ▶ Device independent key distribution



# Outline

Physical principles

Components of computation

Grover's algorithm





# Physical principles



# Physical principles

- ▶ Causality



# Physical principles

- ▶ Causality
- ▶ Purification and purity preservation

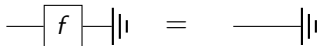


## Physical principles

- ▶ Causality
- ▶ Purification and purity preservation
- ▶ Strong symmetry and pure and perfectly distinguishable states

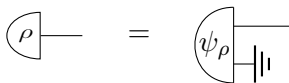


## Physical principle 1: Causality

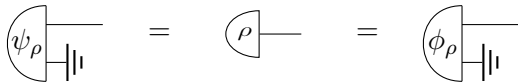




## Physical principle 2: Purification and purity preservation

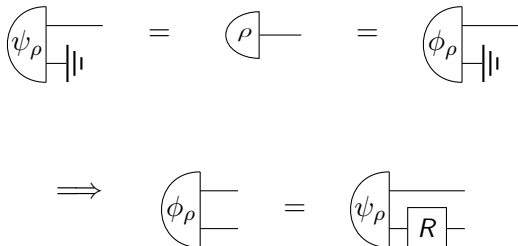


## Physical principle 2: Purification and purity preservation



The diagram shows an equality between three circuit-like expressions. The first expression is a semi-circle on the left containing the symbol  $\psi_\rho$ , with a horizontal line extending to the right from its top edge and two vertical lines extending downwards from its bottom edge. This is followed by an equals sign. The second expression is a semi-circle on the left containing the symbol  $\rho$ , with a horizontal line extending to the right from its top edge. This is followed by another equals sign. The third expression is a semi-circle on the left containing the symbol  $\phi_\rho$ , with a horizontal line extending to the right from its top edge and two vertical lines extending downwards from its bottom edge.

## Physical principle 2: Purification and purity preservation







## Physical principle 3: Strong symmetry and the existence of pure and perfectly distinguishable states

There exists

$$\left\{ \left| i \right\rangle \right\}_{i=0}^n \quad \text{and} \quad \left\{ \left| -j \right\rangle \right\}_{j=0}^n$$



## Physical principle 3: Strong symmetry and the existence of pure and perfectly distinguishable states

There exists

$$\left\{ \left( \begin{array}{c} \circ \\ | \\ i \\ | \\ \circ \end{array} \right) \right\}_{i=0}^n \quad \text{and} \quad \left\{ \left( \begin{array}{c} \circ \\ | \\ -j \\ | \\ \circ \end{array} \right) \right\}_{j=0}^n$$

such that

$$\left( \begin{array}{c} \circ \\ | \\ i \\ | \\ \circ \end{array} \right) \left( \begin{array}{c} \circ \\ | \\ -j \\ | \\ \circ \end{array} \right) = \delta_{ij}$$

## Physical principle 3: Strong symmetry and the existence of pure and perfectly distinguishable states

There exists

$$\left\{ \begin{array}{|c} \text{ } \\ \hline i \\ \hline \end{array} \right\}_{i=0}^n \text{ and } \left\{ \begin{array}{|c} \text{ } \\ \hline -j \\ \hline \end{array} \right\}_{j=0}^n$$

such that

$$\begin{array}{|c} \text{ } \\ \hline i \\ \hline \end{array} \begin{array}{|c} \text{ } \\ \hline j \\ \hline \end{array} = \delta_{ij}$$

Where

$$\left\{ \begin{array}{|c} \text{ } \\ \hline i \\ \hline \end{array} \right\}_{i=0}^n \text{ and } \left\{ \begin{array}{|c} \text{ } \\ \hline i \\ \hline \end{array} \right\}_{i=0}^n$$

## Physical principle 3: Strong symmetry and the existence of pure and perfectly distinguishable states

There exists

$$\left\{ \begin{array}{|c} \text{ } \\ \hline i \\ \hline \text{ } \end{array} \right\}_{i=0}^n \text{ and } \left\{ \begin{array}{|c} \text{ } \\ \hline -j \\ \hline \text{ } \end{array} \right\}_{j=0}^n$$

such that

$$\begin{array}{|c} \text{ } \\ \hline i \\ \hline \text{ } \end{array} \begin{array}{|c} \text{ } \\ \hline j \\ \hline \text{ } \end{array} = \delta_{ij}$$

Where

$$\left\{ \begin{array}{|c} \text{ } \\ \hline i \\ \hline \text{ } \end{array} \right\}_{i=0}^n \text{ and } \left\{ \begin{array}{|c} \text{ } \\ \hline i \\ \hline \text{ } \end{array} \right\}_{i=0}^n$$

are related by

$$\begin{array}{|c} \text{ } \\ \hline i \\ \hline \text{ } \end{array} \boxed{T} = \begin{array}{|c} \text{ } \\ \hline i \\ \hline \text{ } \end{array}$$



Do they restrict us to quantum theory?



## Do they restrict us to quantum theory?

- ▶ Real and fermionic quantum theory

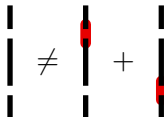


## Do they restrict us to quantum theory?

- ▶ Real and fermionic quantum theory
- ▶ Higher order interference

# Do they restrict us to quantum theory?

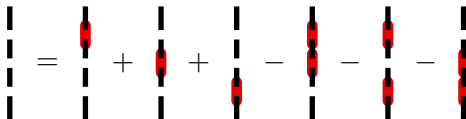
- ▶ Real and fermionic quantum theory
- ▶ Higher order interference





## Do they restrict us to quantum theory?

- ▶ Real and fermionic quantum theory
- ▶ Higher order interference

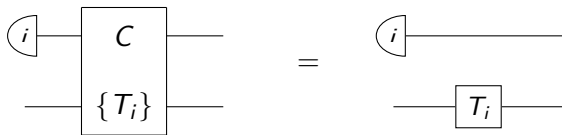




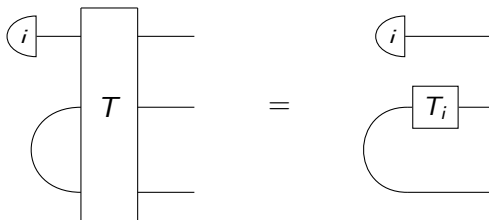
# Component 1: Reversible controlled transformations

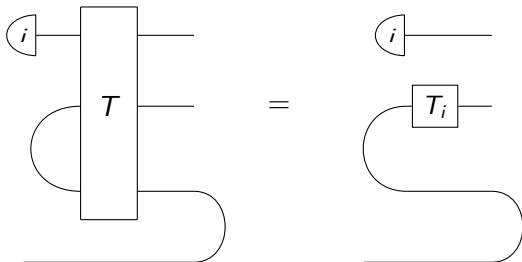


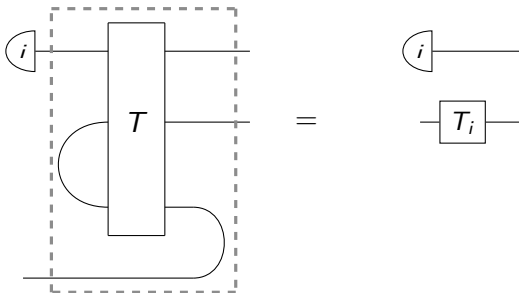
## Component 1: Reversible controlled transformations













## Component 2: Reversible phase transformations

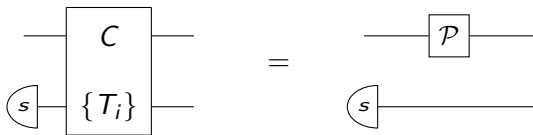
$$\text{---} \square \mathcal{P} \text{---} \text{---} \text{D} i = \text{---} \text{D} i$$

The diagram shows an equality between two circuit components. On the left, a horizontal line enters a square box labeled  $\mathcal{P}$  from the left, and a horizontal line exits the box to the right, entering a semi-circular component labeled  $i$  from the left. On the right, a single horizontal line enters a semi-circular component labeled  $i$  from the left. An equals sign is placed between the two diagrams.





## Component 3: Phase kick-back algorithm





# Grover's algorithm



# Grover's algorithm

- ▶ Important quantum algorithm



# Grover's algorithm

- ▶ Important quantum algorithm
- ▶ Provable advantage



# Grover's algorithm

- ▶ Important quantum algorithm
- ▶ Provable advantage
- ▶ Provably optimal



# Grover's algorithm

- ▶ Important quantum algorithm
- ▶ Provable advantage
- ▶ Provably optimal
- ▶ Oracle problem



## The search problem

*“Given an  $N$  element unstructured list with a unknown marked item  $x$ . Then given an oracle  $\mathcal{O}_x$  how many queries of  $\mathcal{O}_x$  are needed to find  $x$  with high probability?”*



# Quantum oracles



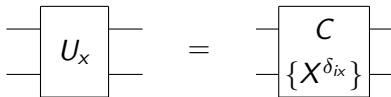


# Quantum oracles

$$U_x |i\rangle |j\rangle = |i\rangle |j \oplus \delta_{ix}\rangle$$

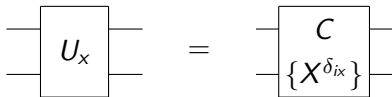
# Quantum oracles

$$U_x |i\rangle |j\rangle = |i\rangle |j \oplus \delta_{ix}\rangle$$



## Quantum oracles

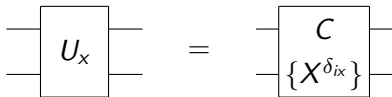
$$U_x |i\rangle |j\rangle = |i\rangle |j \oplus \delta_{ix}\rangle$$



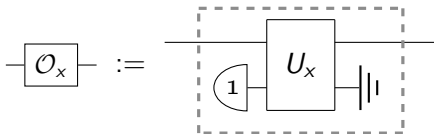
$$\mathcal{O}_x |i\rangle = (-1)^{\delta_{xi}} |i\rangle$$

# Quantum oracles

$$U_x |i\rangle |j\rangle = |i\rangle |j \oplus \delta_{ix}\rangle$$



$$\mathcal{O}_x |i\rangle = (-1)^{\delta_{xi}} |i\rangle$$





## General oracles

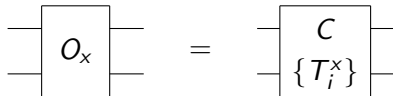


# General oracles

Controlled transformation

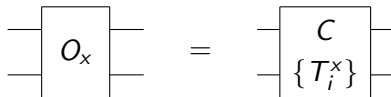
## General oracles

Controlled transformation



## General oracles

Controlled transformation

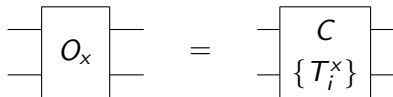


Phase transformation

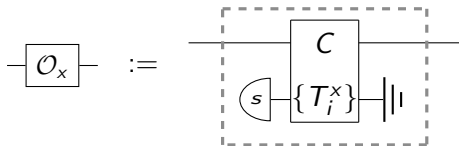


# General oracles

Controlled transformation



Phase transformation





## The lower bound

- ▶ Classical computers:  $O(N)$  queries



## The lower bound

- ▶ Classical computers:  $O(N)$  queries
- ▶ Quantum computers:  $O(\sqrt{N})$  queries



# The quantum speed up



# The quantum speed up

- ▶ Quantum interference provides the speed up?



## The quantum speed up

- ▶ Quantum interference provides the speed up?
- ▶ More interference gives more of a speed up, e.g.  $O(N^{\frac{1}{h}})$ ?

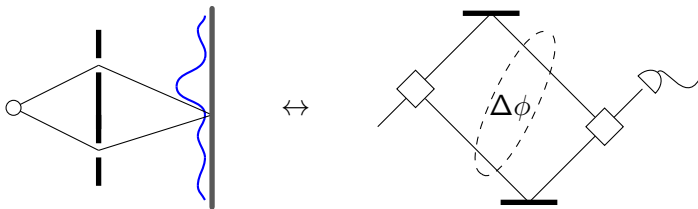


## The quantum speed up

- ▶ Quantum interference provides the speed up?
- ▶ More interference gives more of a speed up, e.g.  $O(N^{\frac{1}{h}})$ ?
- ▶ Interference and phases

# The quantum speed up

- ▶ Quantum interference provides the speed up?
- ▶ More interference gives more of a speed up, e.g.  $O(N^{\frac{1}{\hbar}})$ ?
- ▶ Interference and phases







## Our result

- ▶ Classical computers:  $O(N)$  queries
- ▶ Quantum computers:  $O(\sqrt{N})$  queries



## Our result

- ▶ Classical computers:  $O(N)$  queries
- ▶ Quantum computers:  $O(\sqrt{N})$  queries
- ▶ Computers satisfying our principles:  $\Omega(\sqrt{N/h})$  queries



# Conclusion



## Conclusion

- ▶ Physical principles



# Conclusion

- ▶ Physical principles
  - elementary components of computation



# Conclusion

- ▶ Physical principles
  - elementary components of computation
  - the quantum lower bound



## Conclusion

- ▶ Physical principles
  - elementary components of computation
  - the quantum lower bound
- ▶ Do we need all of these principles?



## Conclusion

- ▶ Physical principles
  - elementary components of computation
  - the quantum lower bound
- ▶ Do we need all of these principles?
- ▶ Can we reach this lower bound?





## Conclusion

- ▶ Physical principles
  - elementary components of computation
  - the quantum lower bound
- ▶ Do we need all of these principles?
- ▶ Can we reach this lower bound?
- ▶ Practical applications?