A Complete Equational Theory for Quantum Circuits

Alexandre Clément[*‡], Nicolas Heurtel[†‡], Shane Mansfield[†], Simon Perdrix[*], Benoît Valiron[‡¶]

[*]Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France
[†]Quandela, 7 rue Léonard de Vinci, 91300 Massy, France
[‡]Université Paris-Saclay, Inria, CNRS, ENS Paris-Saclay, LMF, 91190, Gif-sur-Yvette, France
[¶]CentraleSupélec, 91190, Gif-sur-Yvette, France

LICS 2023

June 29, 2023

Quantum Circuits

- Roughly speaking, they are the assembly language of a quantum processor.
- Therefore ubiquitous in quantum computing.

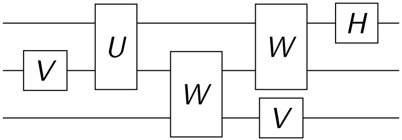
Quantum Circuits

- Roughly speaking, they are the assembly language of a quantum processor.
- Therefore ubiquitous in quantum computing.

Quantum Circuits

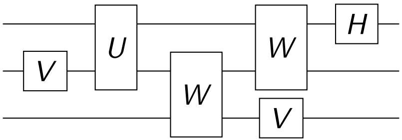
- Roughly speaking, they are the assembly language of a quantum processor.
- Therefore ubiquitous in quantum computing.

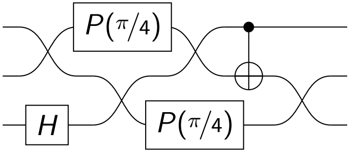
- Roughly speaking, they are the assembly language of a quantum processor.
- Therefore ubiquitous in quantum computing.



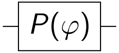
Quantum Circuits

- Roughly speaking, they are the assembly language of a quantum processor.
- Therefore ubiquitous in quantum computing.



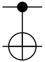


We consider the PROP of quantum circuits generated by:



phase gate
($\simeq$ Z-rotation)

Hadamard



controlled
not

Structure of PROP:

- Additional generators:

empty
circuit

identity

swap

- The circuits are built by means of:

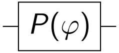
sequential
composition
$C_2 \circ C_1$

parallel
composition
$C_1 \otimes C_2$

- Deformation rules, e.g.

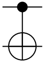
Quantum Circuits

We consider the PROP of quantum circuits generated by:



phase gate
($\simeq$ Z-rotation)

Hadamard



controlled
not

Structure of PROP:

- Additional generators:

empty
circuit

identity

swap

- The circuits are built by means of:

sequential
composition
$C_2 \circ C_1$

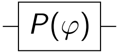
parallel
composition
$C_1 \otimes C_2$

- Deformation rules, e.g.

=

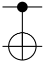
Quantum Circuits

We consider the PROP of quantum circuits generated by:



phase gate
($\simeq$ Z-rotation)

Hadamard



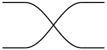
controlled
not

Structure of PROP:

- Additional generators:

empty
circuit

identity



swap

- The circuits are built by means of:

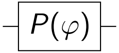
sequential
composition
$C_2 \circ C_1$

parallel
composition
$C_1 \otimes C_2$

- Deformation rules, e.g.

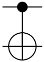
Quantum Circuits

We consider the PROP of quantum circuits generated by:



phase gate
($\simeq Z$-rotation)

Hadamard



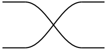
controlled
not

Structure of PROP:

- Additional generators:

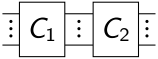
empty
circuit

identity

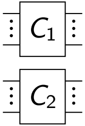


swap

- The circuits are built by means of:



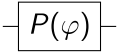
sequential
composition
$C_2 \circ C_1$



parallel
composition
$C_1 \otimes C_2$

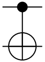
- Deformation rules, e.g.

We consider the PROP of quantum circuits generated by:



phase gate
(≃ Z-rotation)

Hadamard



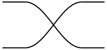
controlled
not

Structure of PROP:

- Additional generators:

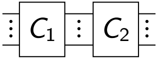
empty
circuit

identity

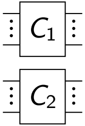


swap

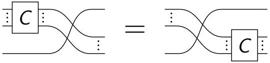
- The circuits are built by means of:



sequential
composition
$C_2 \circ C_1$



parallel
composition
$C_1 \otimes C_2$

- Deformation rules, e.g. 

We consider the PROP of quantum circuits generated by:

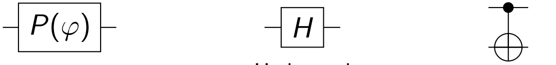
phase gate ($\simeq$ Z-rotation) | Hadamard | controlled not

We define:

A. Barenco *et al.*, *Elementary gates for quantum computation*, 1995.

Quantum Circuits

We consider the PROP of quantum circuits generated by:



phase gate (≃ Z-rotation) — Hadamard — controlled not

We define:

$Z := P(\pi)$ $\quad$ $X := H\,Z\,H$ $\quad$ $R_X(\theta) := H\,P(\theta)\,H$

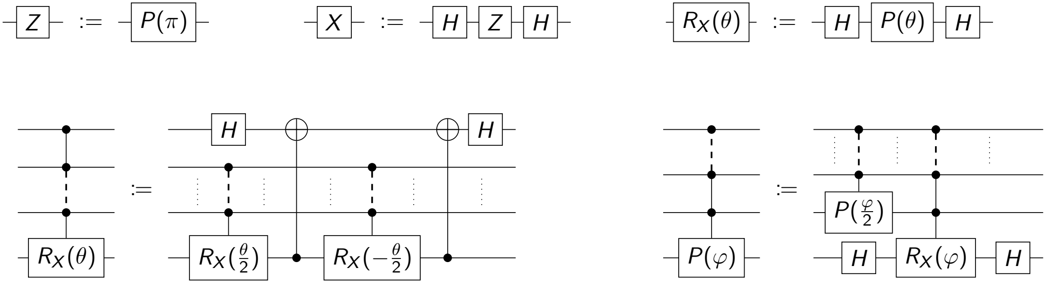
A. Barenco *et al.*, *Elementary gates for quantum computation*, 1995.

Quantum Circuits

We consider the PROP of quantum circuits generated by:

phase gate (≃ Z-rotation) | Hadamard | controlled not

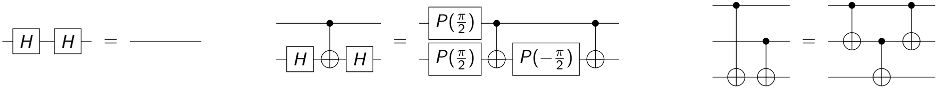
We define:



A. Barenco *et al.*, *Elementary gates for quantum computation*, 1995.

Equational Theories for Quantum Circuits

An equational theory is a set of equalities between circuits, e.g.:



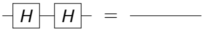
- Common tool for doing circuit transformations
- Used in particular for circuit optimisation

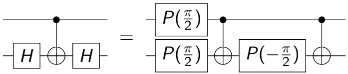
It is complete if any two circuits representing the same unitary can be transformed into each other.

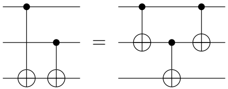
- Provides theoretical foundations e.g. for defining rewriting strategies
- Open problem for 30 years

Equational Theories for Quantum Circuits

An equational theory is a set of equalities between circuits, e.g.:







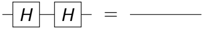
- Common tool for doing circuit transformations
- Used in particular for circuit optimisation

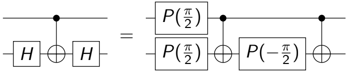
It is complete if any two circuits representing the same unitary can be transformed into each other.

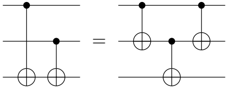
- Provides theoretical foundations e.g. for defining rewriting strategies
- Open problem for 30 years

Equational Theories for Quantum Circuits

An equational theory is a set of equalities between circuits, e.g.:





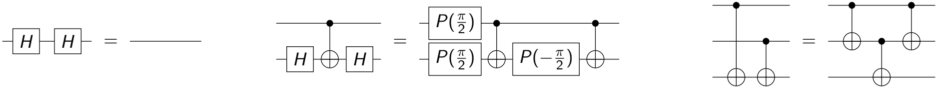


- Common tool for doing circuit transformations
- Used in particular for circuit optimisation

It is complete if any two circuits representing the same unitary can be transformed into each other.

- Provides theoretical foundations e.g. for defining rewriting strategies
- Open problem for 30 years

An equational theory is a set of equalities between circuits, e.g.:



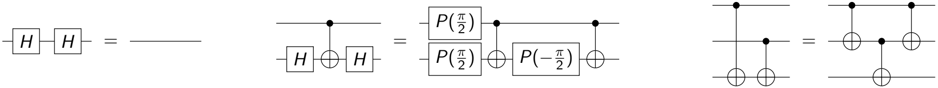
- Common tool for doing circuit transformations
- Used in particular for circuit optimisation

It is complete if any two circuits representing the same unitary can be transformed into each other.

- Provides theoretical foundations e.g. for defining rewriting strategies
- Open problem for 30 years

Equational Theories for Quantum Circuits

An equational theory is a set of equalities between circuits, e.g.:



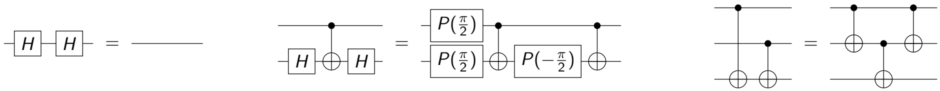
- Common tool for doing circuit transformations
- Used in particular for circuit optimisation

It is complete if any two circuits representing the same unitary can be transformed into each other.

- Provides theoretical foundations e.g. for defining rewriting strategies
- Open problem for 30 years

Equational Theories for Quantum Circuits

An equational theory is a set of equalities between circuits, e.g.:



- Common tool for doing circuit transformations
- Used in particular for circuit optimisation

It is complete if any two circuits representing the same unitary can be transformed into each other.

- Provides theoretical foundations e.g. for defining rewriting strategies
- Open problem for 30 years

Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m\times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m \times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m\times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m\times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m \times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

Partial Results

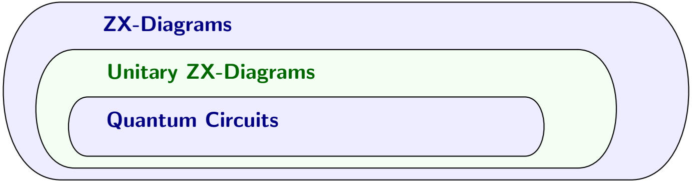
- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m \times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m\times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

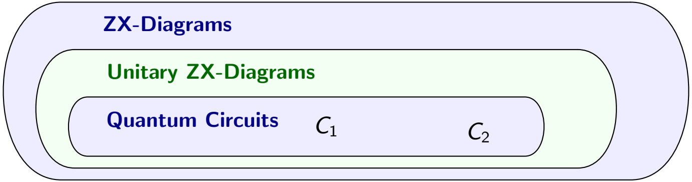
Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m \times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.



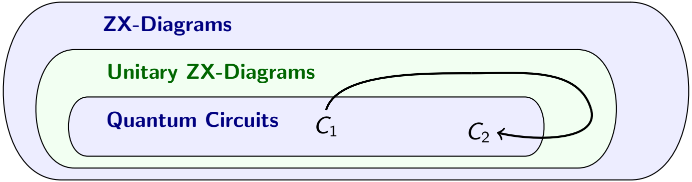
Partial Results

- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m \times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.

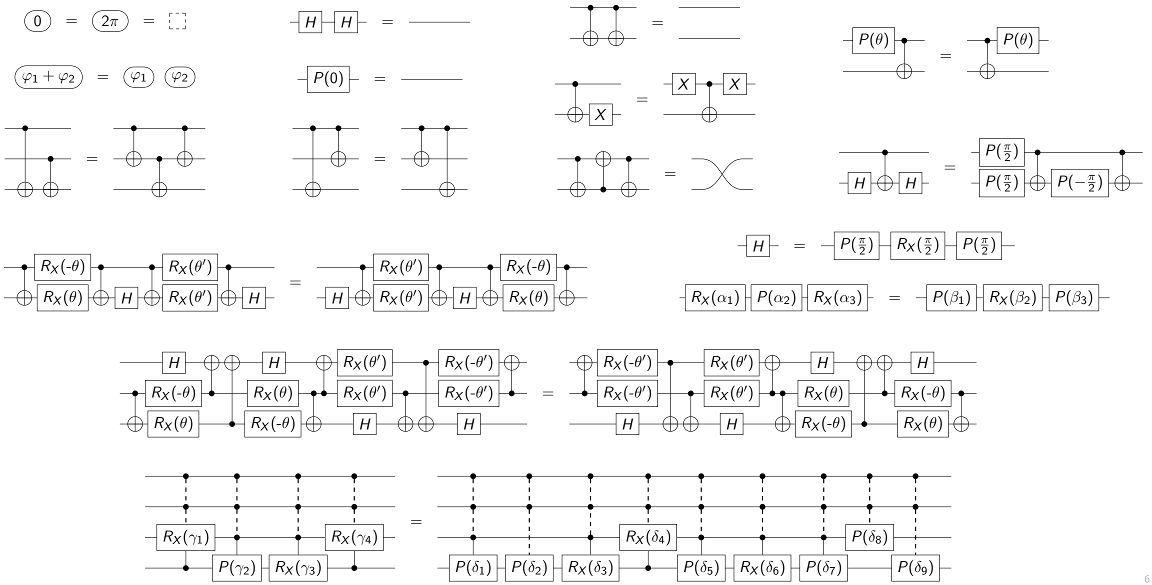


Partial Results

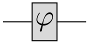
- Complete equational theories for non-universal fragments, e.g.:
  - circuits on at most 2 qubits [X. Bian, P. Selinger, '18]
  - stabilizer circuits [A. Ranchin, B. Coecke, '14, J. Makary, N. J. Ross, P. Selinger, '21]
  - CNot-dihedral circuits [M. Amy, J. Chen, N. J. Ross, '18]
- ZX-calculus: generalisation of quantum circuits
  - more expressive than quantum circuits (can represent all matrices in $\mathbb{C}^{m\times n}$)
  - equipped with a complete equational theory [E. Jeandel, S. Perdrix, R. Vilmart, '18]
  - extracting a quantum circuit from a unitary ZX-diagram is $\#P$-hard in general
  - completeness of ZX-calculus does not lead to completeness inside quantum circuits.



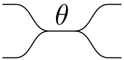
A Complete Equational Theory for Quantum Circuits



LOPP-circuits are generated by:



phase shifter



beam splitter

together with:

by means of:

sequential composition

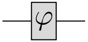
$D_2 \circ D_1$

parallel composition

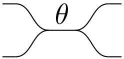
$D_1 \oplus D_2$

Structure of PROP

LOPP-circuits are generated by:

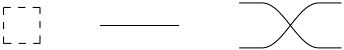


phase shifter

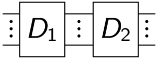


beam splitter

together with:

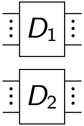


by means of:



sequential composition

$D_2 \circ D_1$

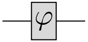


parallel composition

$D_1 \oplus D_2$

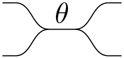
Structure of PROP

LOPP-circuits are generated by:



phase shifter

$e^{i\varphi}$



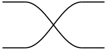
beam splitter

$$\begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$$

together with:

$()$

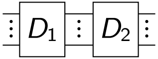
1



$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

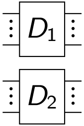
Structure of PROP

by means of:



sequential composition

$D_2 \circ D_1$



parallel composition

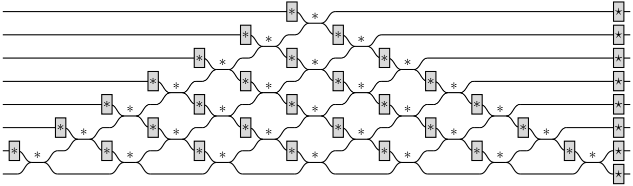
$D_1 \oplus D_2$

$$\left(\begin{array}{c|c} [\![D_1]\!] & 0 \\ \hline 0 & [\![D_2]\!] \end{array}\right)$$

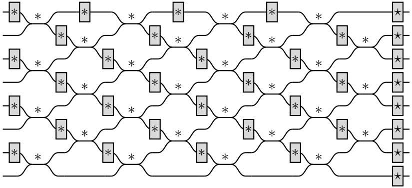
Universality of LOPP-Circuits

Proposition

For any unitary $U \in \mathbb{C}^{n\times n}$, there exists a LOPP-circuit D such that $[\![D]\!] = U$.

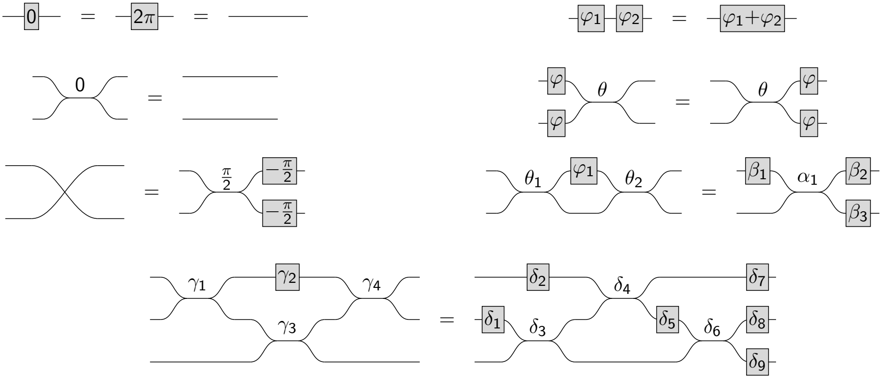


Reck *et al.* (1994)



Clements *et al.* (2016)

Complete Equational Theory for LOPP-Circuits



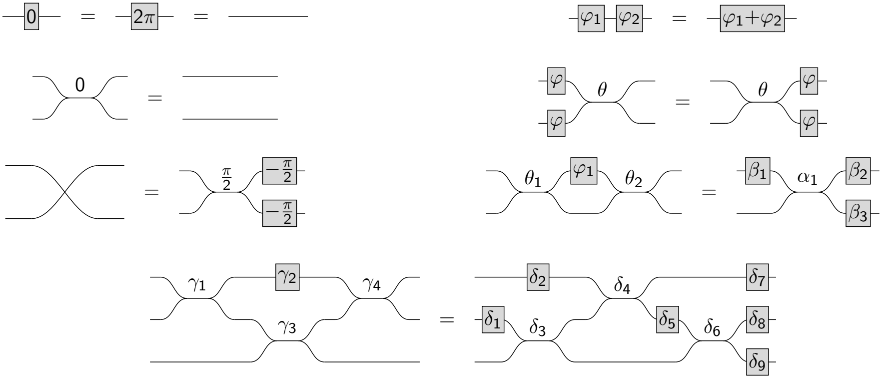
Proposition (Soundness)

$\forall D_1, D_2$, if $\text{LOPP} \vdash D_1 = D_2$ then $[\![D_1]\!] = [\![D_2]\!]$.

Theorem (Completeness)

$\forall D_1, D_2$, *if* $[\![D_1]\!] = [\![D_2]\!]$ *then* $\text{LOPP} \vdash D_1 = D_2$.

Complete Equational Theory for LOPP-Circuits



Proposition (Soundness)

$\forall D_1, D_2$, if $\mathrm{LOPP} \vdash D_1 = D_2$ then $[\![D_1]\!] = [\![D_2]\!]$.

Theorem (Completeness)

$\forall D_1, D_2$, *if* $[\![D_1]\!] = [\![D_2]\!]$ *then* $\mathrm{LOPP} \vdash D_1 = D_2$.

Proof of Completeness

Proposition (Universality of LOPP)

For any unitary $U \in \mathbb{C}^{n\times n}$, there exists a LOPP-circuit D such that $[\![D]\!] = U$.

Proposition (Universality of QC)

For any unitary $U \in \mathbb{C}^{2^n\times 2^n}$, there exists a quantum circuit C such that $[\![C]\!] = U$.

Proof of Completeness

Proposition (Universality of LOPP)

For any unitary $U \in \mathbb{C}^{n\times n}$, there exists a LOPP-circuit D such that $[\![D]\!] = U$.

Proposition (Universality of QC)

For any unitary $U \in \mathbb{C}^{2^n\times 2^n}$, there exists a quantum circuit C such that $[\![C]\!] = U$.

n-Qubit Quantum Circuits

C_1 C_2

2^n-Mode Optical Circuits

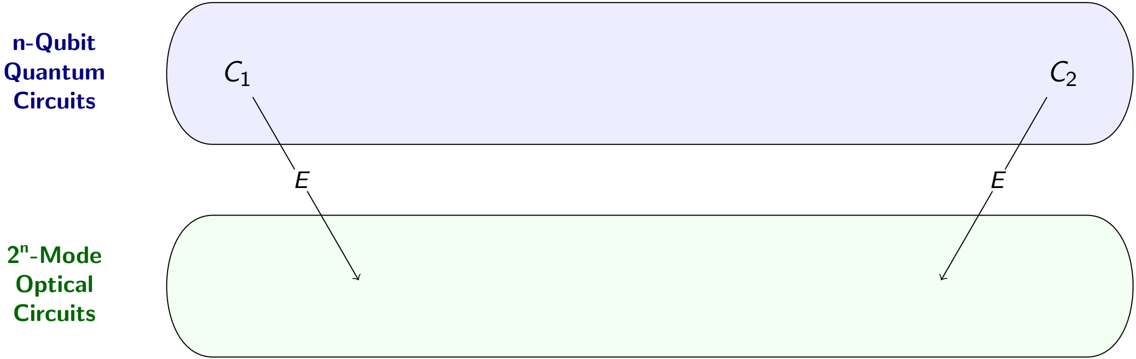
Proof of Completeness

Proposition (Universality of LOPP)

For any unitary $U \in \mathbb{C}^{n\times n}$, there exists a LOPP-circuit D such that $[\![D]\!] = U$.

Proposition (Universality of QC)

For any unitary $U \in \mathbb{C}^{2^n\times 2^n}$, there exists a quantum circuit C such that $[\![C]\!] = U$.



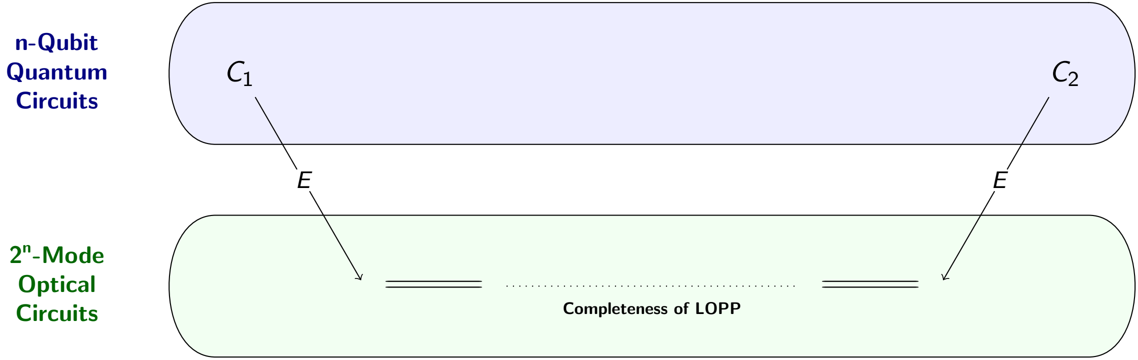
Proof of Completeness

Proposition (Universality of LOPP)

For any unitary $U \in \mathbb{C}^{n\times n}$, there exists a LOPP-circuit D such that $[\![D]\!] = U$.

Proposition (Universality of QC)

For any unitary $U \in \mathbb{C}^{2^n\times 2^n}$, there exists a quantum circuit C such that $[\![C]\!] = U$.



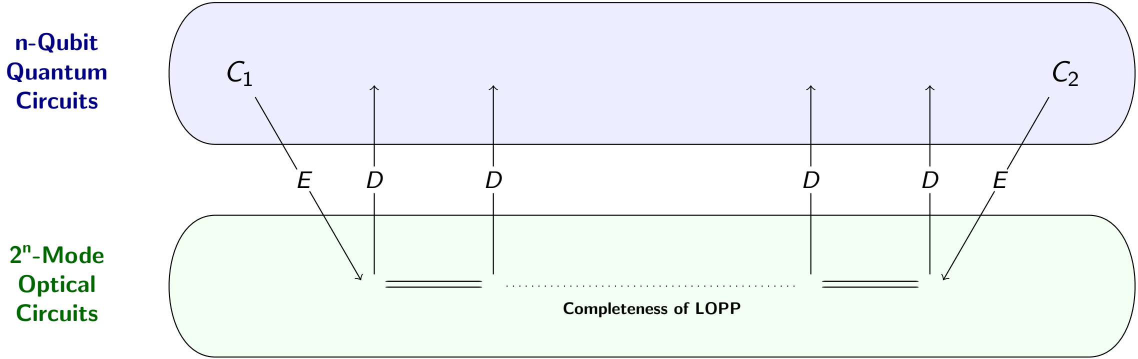
Proof of Completeness

Proposition (Universality of LOPP)

For any unitary $U \in \mathbb{C}^{n\times n}$, there exists a LOPP-circuit D such that $[\![D]\!] = U$.

Proposition (Universality of QC)

For any unitary $U \in \mathbb{C}^{2^n\times 2^n}$, there exists a quantum circuit C such that $[\![C]\!] = U$.



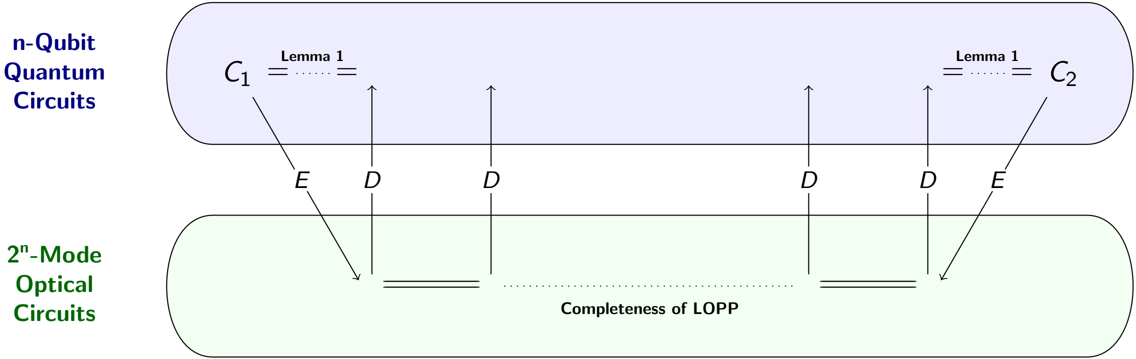
Proof of Completeness

Lemma 1

For any quantum circuit C, $\mathrm{QC} \vdash D(E(C)) = C$.

Lemma 2

For every equation of the LOPP-calculus, of the form $D_1 = D_2$, *one has* $\mathrm{QC} \vdash D(D_1) = D(D_2)$.



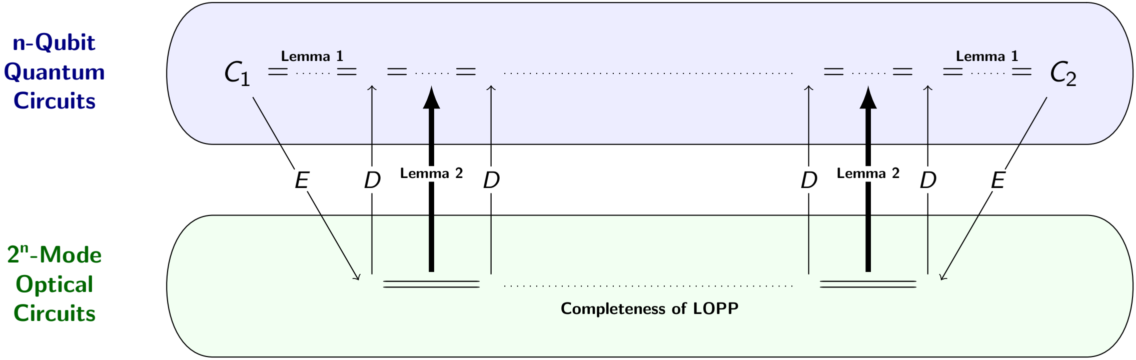
Proof of Completeness

Lemma 1

For any quantum circuit C, $\mathrm{QC} \vdash D(E(C)) = C$.

Lemma 2

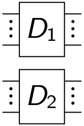
For every equation of the LOPP-calculus, of the form $D_1 = D_2$, *one has* $\mathrm{QC} \vdash D(D_1) = D(D_2)$.



Key Aspects of the Proof

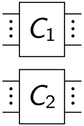
- Note that optical circuits and quantum circuits have different structures:

Optical circuits:



$D_1 \oplus D_2$

Quantum circuits:



$C_1 \otimes C_2$

$\Rightarrow$ To define E and D, we "sequentialise" the circuits:

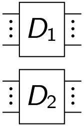
$\Rightarrow$ Some deformation rules need to be treated as proper equations.

- Decoding produces multi-controlled gates, e.g.:

Key Aspects of the Proof

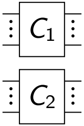
- Note that optical circuits and quantum circuits have different structures:

Optical circuits:



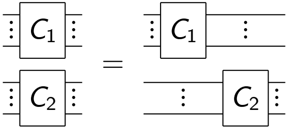
$D_1 \oplus D_2$

Quantum circuits:



$C_1 \otimes C_2$

$\Rightarrow$ To define E and D, we “sequentialise” the circuits:

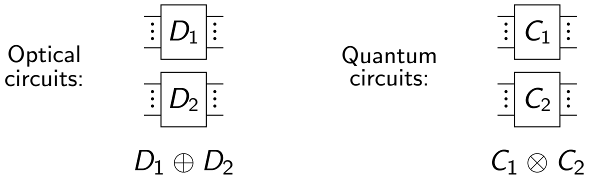


$\Rightarrow$ Some deformation rules need to be treated as proper equations.

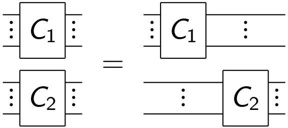
- Decoding produces multi-controlled gates, e.g.:

Key Aspects of the Proof

- Note that optical circuits and quantum circuits have different structures:



$\Rightarrow$ To define E and D, we "sequentialise" the circuits:



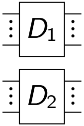
$\Rightarrow$ Some deformation rules need to be treated as proper equations.

- Decoding produces multi-controlled gates, e.g.:

Key Aspects of the Proof

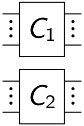
- Note that optical circuits and quantum circuits have different structures:

Optical circuits:



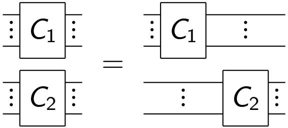
$D_1 \oplus D_2$

Quantum circuits:



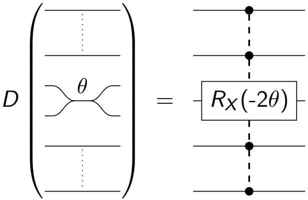
$C_1 \otimes C_2$

$\Rightarrow$ To define E and D, we “sequentialise” the circuits:



$\Rightarrow$ Some deformation rules need to be treated as proper equations.

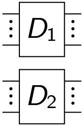
- Decoding produces multi-controlled gates, e.g.:



Key Aspects of the Proof

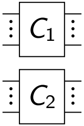
- Note that optical circuits and quantum circuits have different structures:

Optical circuits:



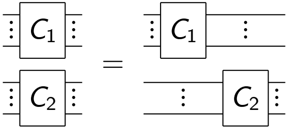
$D_1 \oplus D_2$

Quantum circuits:



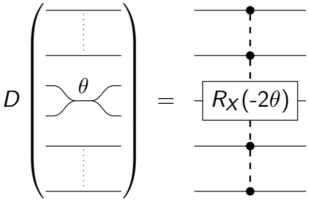
$C_1 \otimes C_2$

$\Rightarrow$ To define E and D, we "sequentialise" the circuits:



$\Rightarrow$ Some deformation rules need to be treated as proper equations.

- Decoding produces multi-controlled gates, e.g.:



$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \cos\theta & i\sin\theta & & \\ & & & i\sin\theta & \cos\theta & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}$$

two-level matrix

Future Work

- Simplify the equational theory, prove minimality
- Design procedures e.g. for circuit optimisation
- Prove upper and lower bounds on the size of the derivations, and of the intermediate circuits

Future Work

- Simplify the equational theory, prove minimality
- Design procedures e.g. for circuit optimisation
- Prove upper and lower bounds on the size of the derivations, and of the intermediate circuits

Future Work

- Simplify the equational theory, prove minimality
- Design procedures e.g. for circuit optimisation
- Prove upper and lower bounds on the size of the derivations, and of the intermediate circuits

Future Work

- Simplify the equational theory, prove minimality
- Design procedures e.g. for circuit optimisation
- Prove upper and lower bounds on the size of the derivations, and of the intermediate circuits