# Quantum Circuit Completeness: Extensions and Simplifications

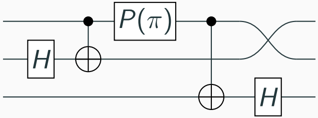
**32nd EACSL Annual Conference on Computer Science Logic 2024 (CSL'24)**

Alexandre Clément*, Noé Delorme‡, Simon Perdrix‡, and Renaud Vilmart*

*Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France
‡Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

# What is it all about?

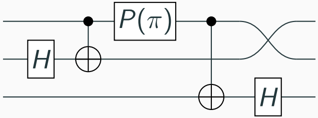
Quantum circuits are a rigourous graphical representation of quantum algorithms.



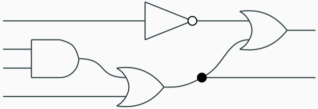

Just like boolean circuits are a rigourous graphical representation of classical algorithms.

# What is it all about?

Quantum circuits are a rigourous graphical representation of quantum algorithms.

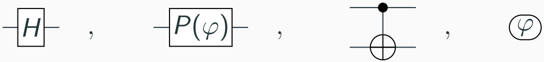



Just like boolean circuits are a rigourous graphical representation of classical algorithms.



# Quantum circuits as a graphical language

Quantum circuits are generated by




and can be composed sequentially with $\circ$ and in parallel with $\otimes$ as



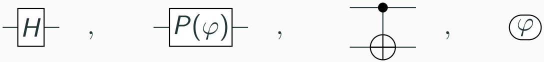
and



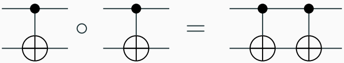

to form new circuits.

# Quantum circuits as a graphical language

Quantum circuits are generated by



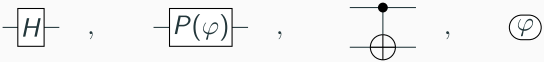

and can be composed sequentially with ∘ and in parallel with ⊗ as



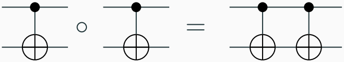
and


to form new circuits.

Quantum circuits are generated by

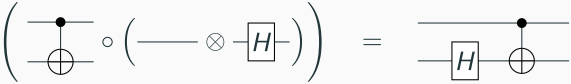



and can be composed sequentially with ∘ and in parallel with ⊗ as



and


to form new circuits.



# Quantum circuits as a graphical language

Formally, graphical languages are defined within the prop formalism with some deformation rules such that


or

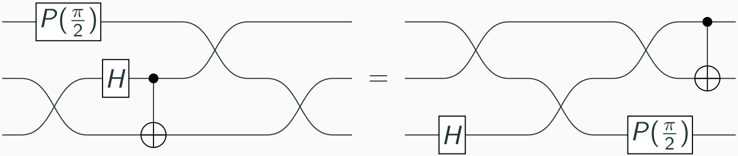

This framework captures the intuitive behaviour of wires by ensuring that circuits are defined "up to deformation".

# Quantum circuits as a graphical language

Formally, graphical languages are defined within the prop formalism with some deformation rules such that


or


This framework captures the intuitive behaviour of wires by ensuring that circuits are defined “up to deformation”.



# Other usual gates as shortcut notations

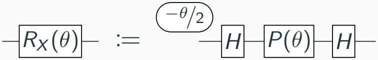
There are only four different kinds of generators

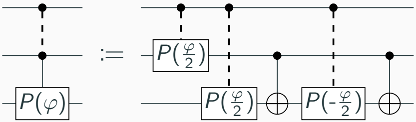

Other gates can be defined as shortcut notations.

# Other usual gates as shortcut notations

There are only four different kinds of generators


Other gates can be defined as shortcut notations.



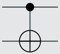
# Standard interpretation of quantum circuits

## Interpretation

$$[\![C_2 \circ C_1]\!] = [\![C_2]\!] \circ [\![C_1]\!] \qquad [\![C_1 \otimes C_2]\!] = [\![C_1]\!] \otimes [\![C_2]\!]$$

$$[\![\;\square\;]\!] = (1) \qquad [\![\;\textcircled{\varphi}\;]\!] = (e^{i\varphi})$$

$$[\![\;-\!\!-\!\!-\;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad [\![\;-\boxed{H}-\;]\!] = {}^1\!/\!\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad [\![\;-\boxed{P(\varphi)}-\;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

$[\![$  $]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

$[\![$  $]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

circuits $\neq$ matrices

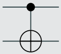
# Standard interpretation of quantum circuits

**Interpretation**

$$[\![ C_2 \circ C_1 ]\!] = [\![ C_2 ]\!] \circ [\![ C_1 ]\!] \qquad [\![ C_1 \otimes C_2 ]\!] = [\![ C_1 ]\!] \otimes [\![ C_2 ]\!]$$

$$[\![ \,\square\, ]\!] = (1) \qquad [\![ \,\textcircled{\varphi}\, ]\!] = (e^{i\varphi})$$

$$[\![ \,-\!\!-\!\!-\, ]\!] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad [\![ -\boxed{H}- ]\!] = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad [\![ -\boxed{P(\varphi)}- ]\!] = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

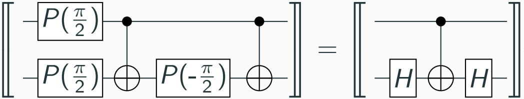
$[\![$  $]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

$[\![$  $]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

circuits $\neq$ matrices

# Motivations

Distinct circuits can have the same interpretation.




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

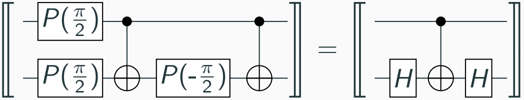
Given a quantum algorithm, which circuit is the best?

**Motivations:**

- Resource optimisation (for instance the number of gates).
- Hardware-constraint satisfaction (for instance topological constraints).
- Verification, circuit equivalence testing.

# Motivations

Distinct circuits can have the same interpretation.



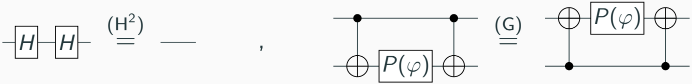

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Given a quantum algorithm, which circuit is the best?

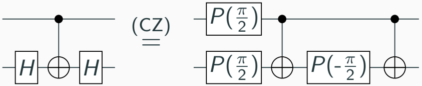
**Motivations:**

- Resource optimisation (for instance the number of gates).
- Hardware-constraint satisfaction (for instance topological constraints).
- Verification, circuit equivalence testing.

We can use simple axioms such that,



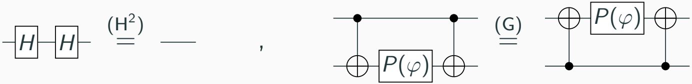

and



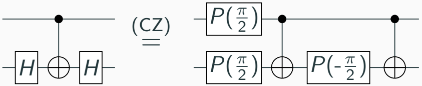

to derive new equations. For instance,

# Using equations to transform circuits

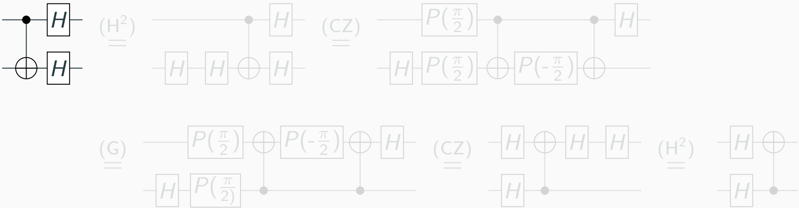
We can use simple axioms such that,




and

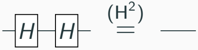



to derive new equations. For instance,

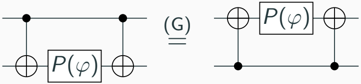


# Using equations to transform circuits

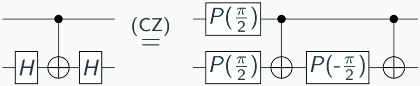
We can use simple axioms such that,



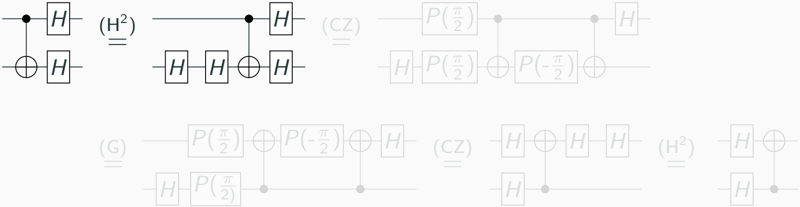

,




and

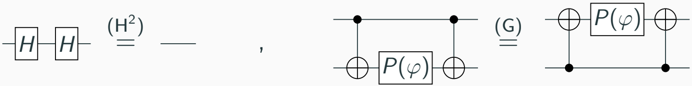



to derive new equations. For instance,

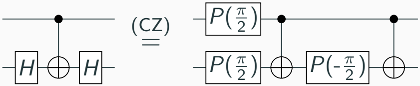


# Using equations to transform circuits

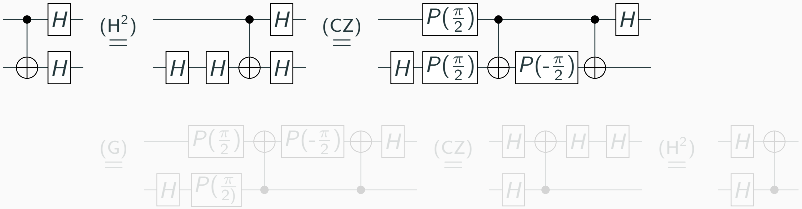
We can use simple axioms such that,




and

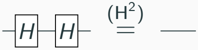



to derive new equations. For instance,

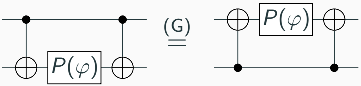


# Using equations to transform circuits

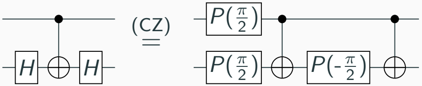
We can use simple axioms such that,



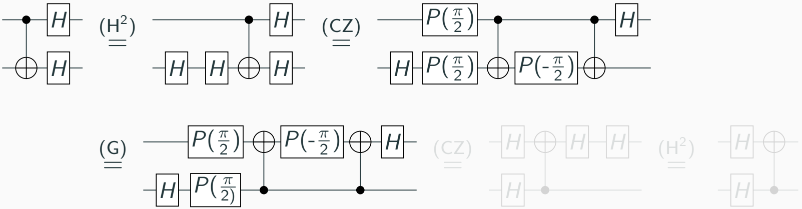

,




and

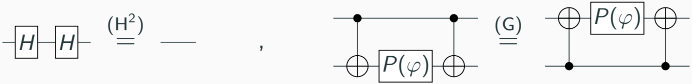



to derive new equations. For instance,

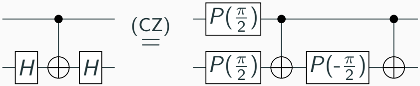


# Using equations to transform circuits

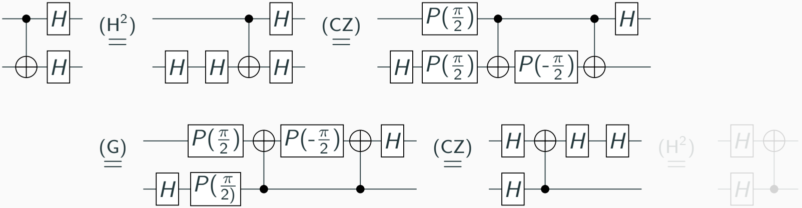
We can use simple axioms such that,




and

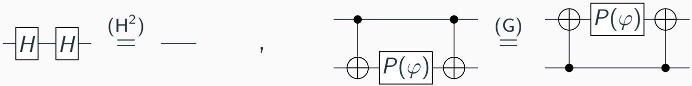



to derive new equations. For instance,

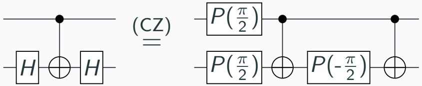


# Using equations to transform circuits

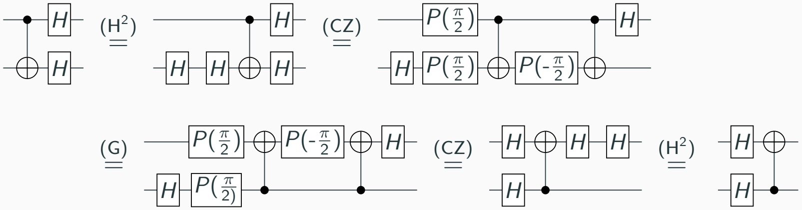
We can use simple axioms such that,




and




to derive new equations. For instance,



# Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) $\Gamma$ from which we can derive any true equation and only true equations?

**Soundness**

Any derivable equation is true.

$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

**Completeness**

Any true equation is derivable.

$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

**Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:**

The first complete and sound equational theory.

# Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) $\Gamma$ from which we can derive any true equation and only true equations?

**Soundness**

Any derivable equation is true.

$$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$$

**Completeness**

Any true equation is derivable.

$$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$$

**Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:**

The first complete and sound equational theory.

# Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) $\Gamma$ from which we can derive any true equation and only true equations?

**Soundness**

Any derivable equation is true.

$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

**Completeness**

Any true equation is derivable.

$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

**Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:**

The first complete and sound equational theory.

# Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) $\Gamma$ from which we can derive any true equation and only true equations?

**Soundness**

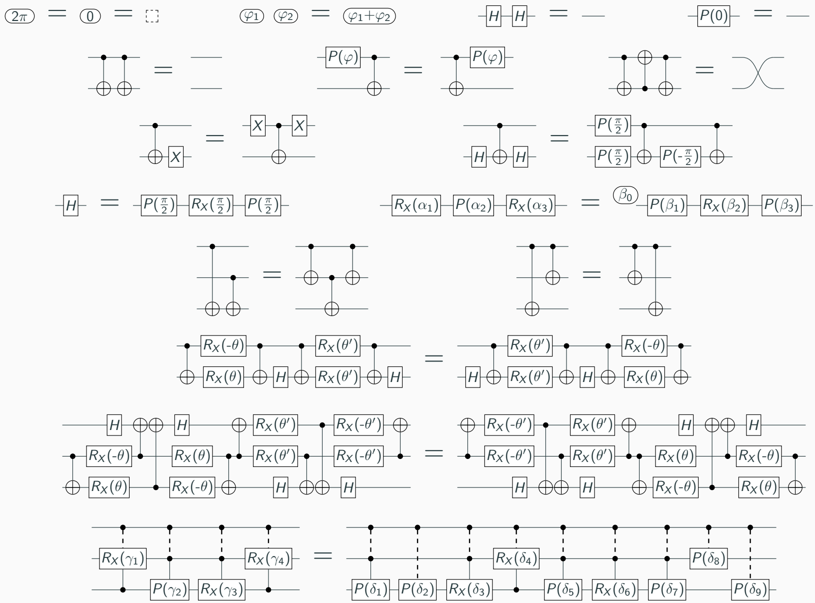
Any derivable equation is true.
$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

**Completeness**

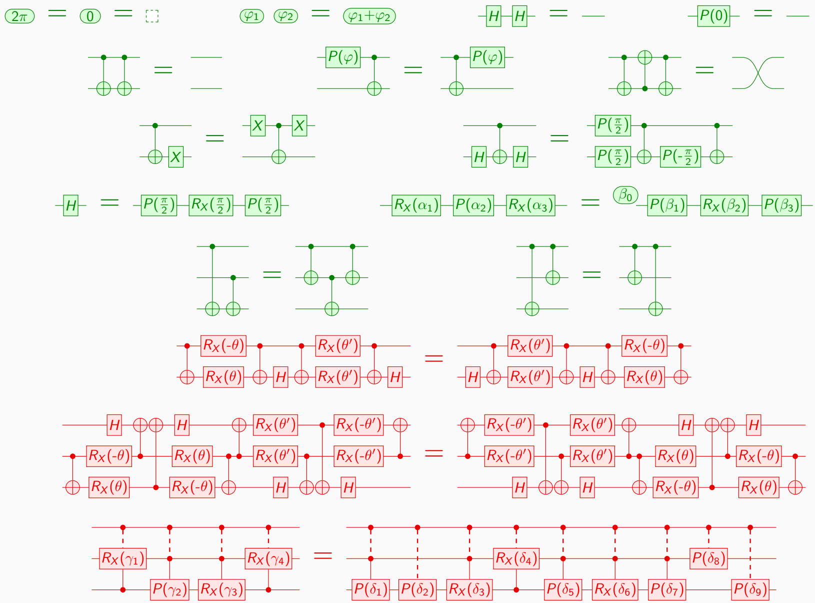
Any true equation is derivable.
$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

**Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:**
The first complete and sound equational theory.

# Complete and sound equational theory [CHMPV LICS'23]



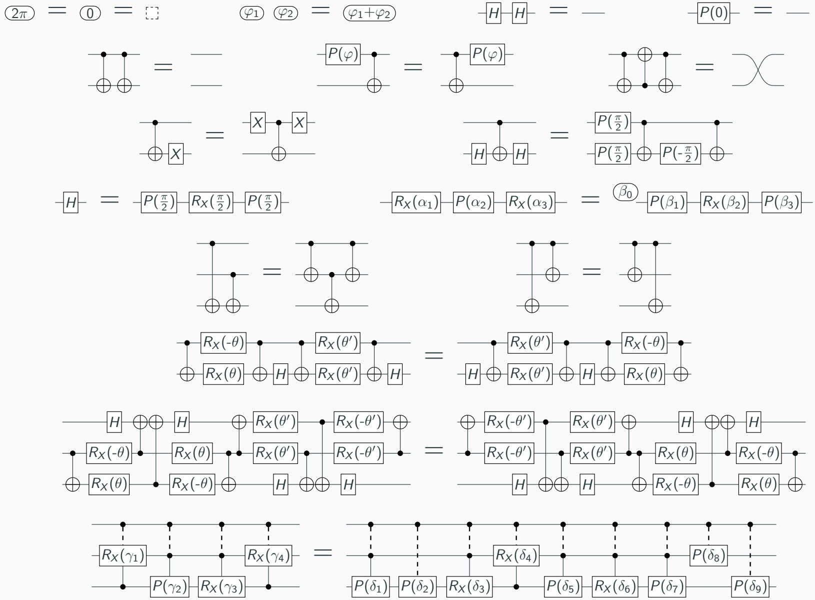
# Some easy and some intricate equations



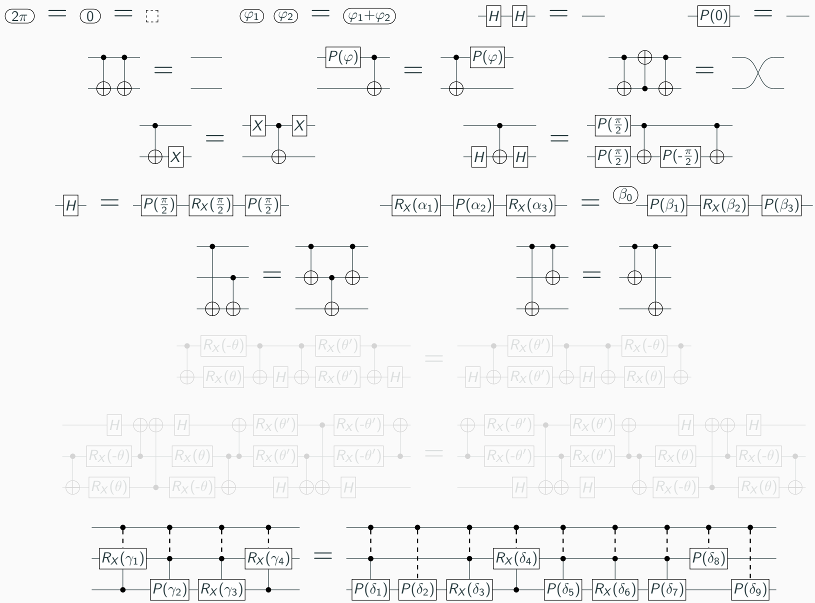
First contribution

# Simplification of the equational theory

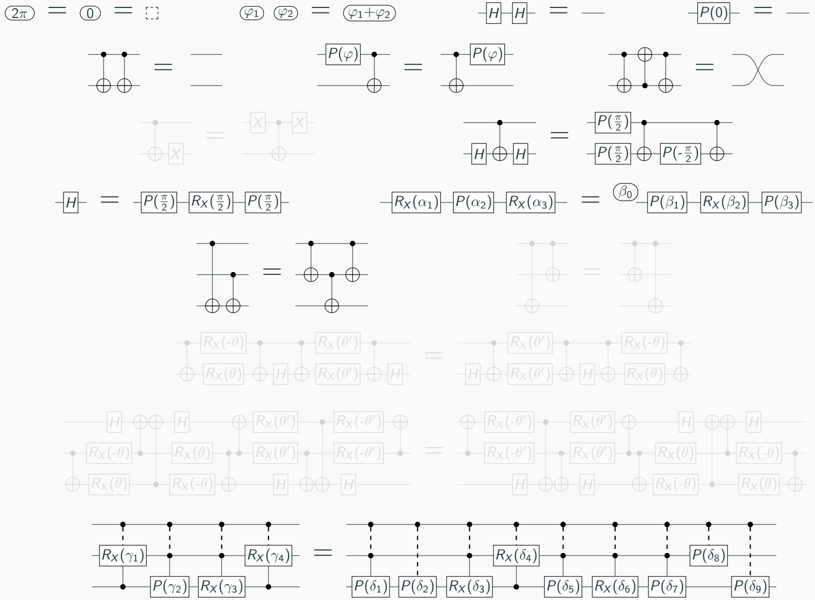
# Simplifications



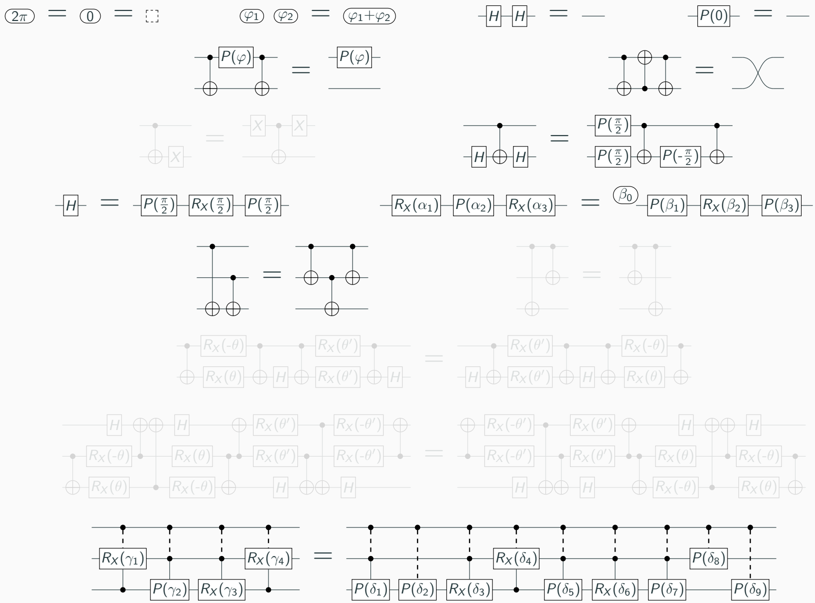
# Simplifications



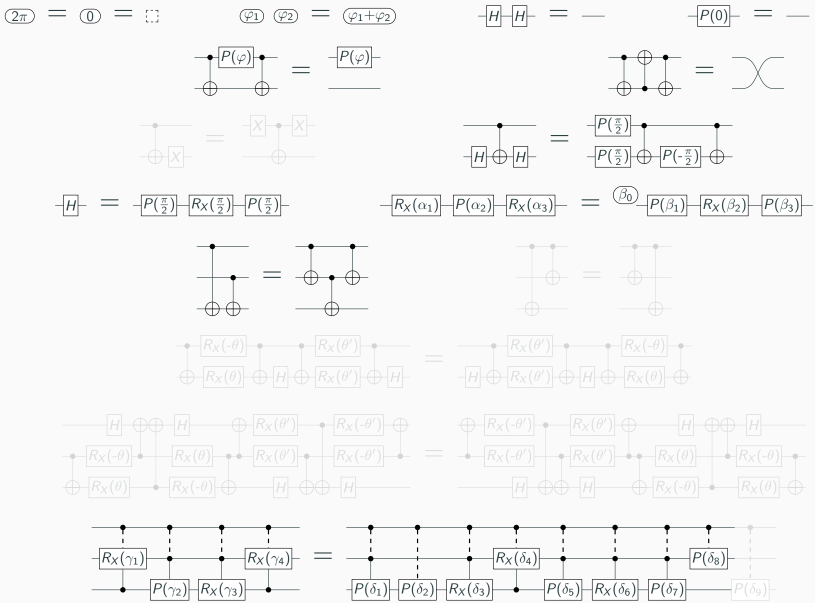
# Simplifications



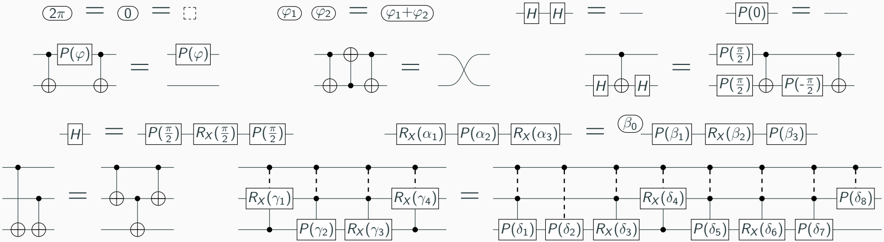
# Simplifications



# Simplifications



# Simplified complete and sound equational theory




**Theorem (Completeness)**

This equational theory is complete, i.e. any two equivalent circuits can be transformed into each other.

Second contribution

# Extension of the equational theory

# Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by


together with

$\vdash$ and $\dashv$

respectively denoting qubit initialisation and qubit destruction.

(The generator $\dashv$ can only be applied to qubits in the $|0\rangle$-state.)

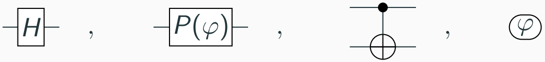
**Semantics**

We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

Universal for isometries

# Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by




together with

$$\vdash \qquad \text{and} \qquad \dashv$$

respectively denoting qubit initialisation and qubit destruction.

(The generator $\dashv$ can only be applied to qubits in the $|0\rangle$-state.)

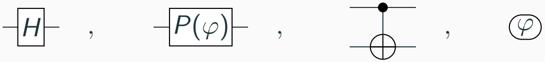
**Semantics**

We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

Universal for isometries

# Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by




together with

$$\vdash \quad \text{and} \quad \dashv$$

respectively denoting qubit initialisation and qubit destruction.

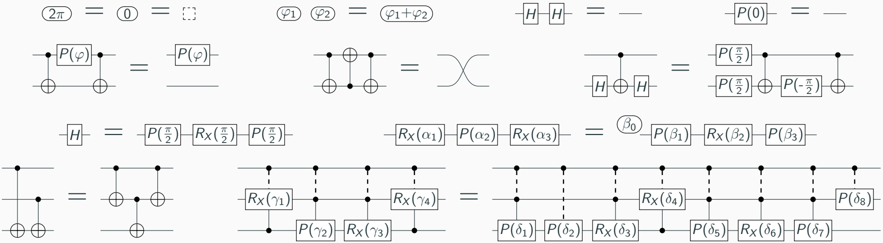
(The generator $\dashv$ can only be applied to qubits in the $|0\rangle$-state.)

**Semantics**

We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

## Universal for isometries

# Equational theory for quantum circuits with ancillae

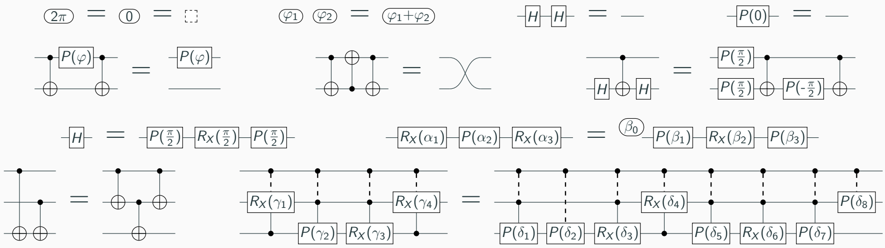


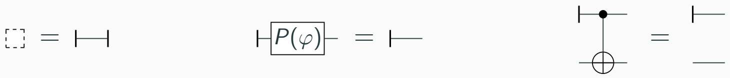


**Theorem (Completeness)**

Adding those three equations makes the equational theory complete for quantum circuits with ancillae.

# Equational theory for quantum circuits with ancillae

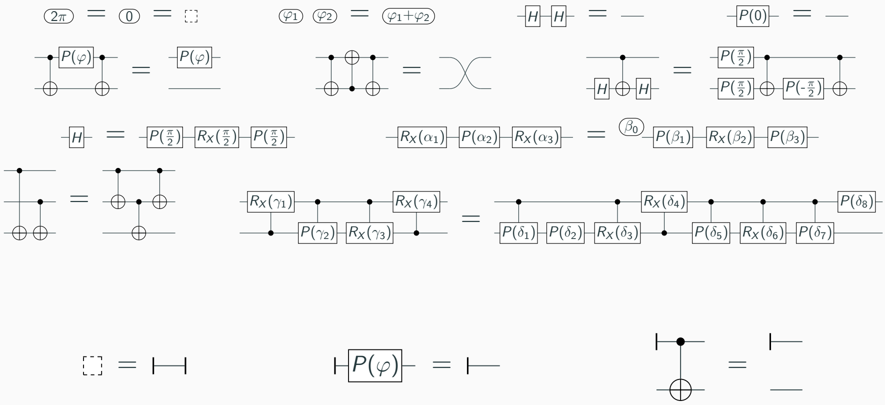



**Theorem (Completeness)**

Adding those three equations makes the equational theory complete for quantum circuits with ancillae.

# Equational theory for quantum circuits with ancillae

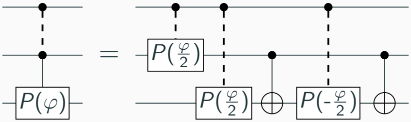


**Proposition**

The big rule can be replaced by its 2-qubits version, leading to an equational theory acting on a bounded number of qubits.

# Alternative definition of multi-controlled gates

Mutli-controlled gates are defined inductively

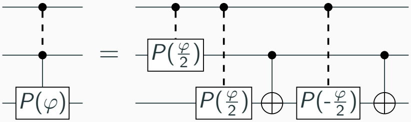



**Problem:** Cannot apply inductive hypothesis as angles are divided by 2.

**Solution:** Using ancillae, we can prove

# Alternative definition of multi-controlled gates

Mutli-controlled gates are defined inductively

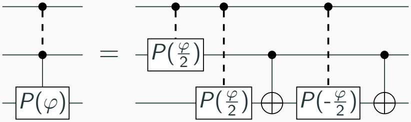



**Problem:** Cannot apply inductive hypothesis as angles are divided by 2.

**Solution:** Using ancillae, we can prove

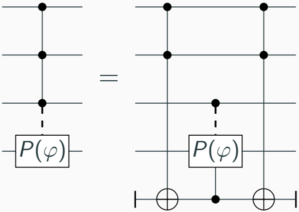
# Alternative definition of multi-controlled gates

Mutli-controlled gates are defined inductively




**Problem:** Cannot apply inductive hypothesis as angles are divided by 2.

**Solution:** Using ancillae, we can prove



# Conclusion

- Simplification of the original equational theory, in particular removed two intricate rules.
- Introducing new techniques to reason on quantum circuits.
- Extension of the completeness result to circuits with ancillae.
- In these extended settings, the equational theory is made only of equations acting on at most 3 qubits.
- Other contribution: extension of the completeness result to circuits with discard (where any qubit can be discarded).

# Conclusion

- Simplification of the original equational theory, in particular removed two intricate rules.
- Introducing new techniques to reason on quantum circuits.
- Extension of the completeness result to circuits with ancillae.
- In these extended settings, the equational theory is made only of equations acting on at most 3 qubits.
- Other contribution: extension of the completeness result to circuits with discard (where any qubit can be discarded).

# Conclusion

- Simplification of the original equational theory, in particular removed two intricate rules.
- Introducing new techniques to reason on quantum circuits.
- Extension of the completeness result to circuits with ancillae.
- In these extended settings, the equational theory is made only of equations acting on at most 3 qubits.
- Other contribution: extension of the completeness result to circuits with discard (where any qubit can be discarded).

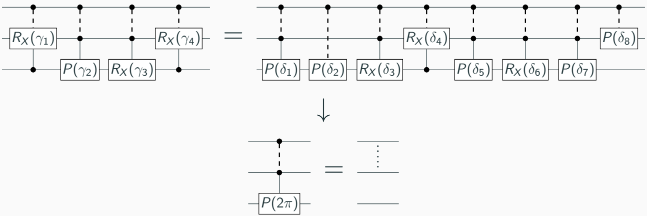
# Conclusion

- Simplification of the original equational theory, in particular removed two intricate rules.
- Introducing new techniques to reason on quantum circuits.
- Extension of the completeness result to circuits with ancillae.
- In these extended settings, the equational theory is made only of equations acting on at most 3 qubits.
- Other contribution: extension of the completeness result to circuits with discard (where any qubit can be discarded).

# Conclusion

- Simplification of the original equational theory, in particular removed two intricate rules.
- Introducing new techniques to reason on quantum circuits.
- Extension of the completeness result to circuits with ancillae.
- In these extended settings, the equational theory is made only of equations acting on at most 3 qubits.
- Other contribution: extension of the completeness result to circuits with discard (where any qubit can be discarded).

Replace the big rule by something simple.



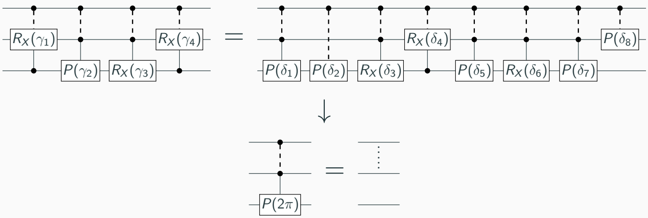

Prove the minimality of the resulting equational theory.

**Theorem (Minimality)**

Each equation of the equational theory is necessary.

# Ongoing work [arXiv:2311.07476]

Replace the big rule by something simple.




Prove the minimality of the resulting equational theory.

**Theorem (Minimality)**

Each equation of the equational theory is necessary.

# Thanks

https://doi.org/10.4230/LIPIcs.CSL.2024.20

**Quantum Circuit Completeness: Extensions and Simplifications**

Alexandre Clément, Noé Delorme, Simon Perdrix, and Renaud Vilmart